Multidimensional Quantum Key Distribution with Single Side Pulse and Single Side Band Modulation Multiplexing

A Thesis
Presented to
The Academic Faculty

by

Olivier L. Guerreau-Lambert

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy

School of Electrical and Computer Engineering
Georgia Institute of Technology
December 2005

Multidimensional Quantum Key Distribution with Single Side Pulse and Single Side Band Modulation Multiplexing

Approved by:

Dr. Steven W. McLaughlin, Advisor
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. John R. Barry
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. François J. Malassenet, Co-Advisor
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. William T. Rhodes
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Faramarz Fekri
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Alex Kuzmich
School of Physics
Georgia Institute of Technology

Date Approved: November 21, 2005

To my parents, yesterday, and tomorrow

for their great support along these years.

ACKNOWLEDGEMENTS

This research work would not have been possible without the help of many people. I would like to take this opportunity to thank my thesis advisors Dr. Steve W. McLaughlin and Dr. François J. Malassenet.

I am thankful for the faculty members serving in my committee, Dr. Faramarz Fekri, Dr. Bill Rhodes, Dr. John Barry, and Dr. Alex Kuzmich.

A special dedication to Thierry, Amandeep, and Achin for great squash games during my time in Georgia Tech CRC.

I would like to thank all the people from the GTL-CNRS Telecom lab, Aurélien, Johan, Matthieu, Fonfred, Xavier, Stéphane, David, Jérôme, Jacky, and also Muriel, Sam, Olivier, Marc, Stéphane, and PAL for the lab *bonne ambiance*.

I would like to especially thank François Malassenet, Georgia Tech Lorraine Director when I was there, Georgia Tech Faculty Member, and Advisor, but most important friend now. This dissertation would not have been the same today without him, neither the guy that wrote it.

Finally, I thank my parents, my sisters, and Stéphanie for their love and great support since kindergarten until the final writing of this dissertation.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

SUMMARY

Communication methods have drastically evolved since the creation of writing. In ancient times, couriers carried written messages between persons directly. Today, people communicate with satellites or underseao optical fiber. An important use of communications includes confidential data–such as military, banking, or personal information–that cannot be transmitted plainly over a classical channel where everybody would be able to read and copy. In ancient times, privacy was guaranteed with empirical systems. For example, around 600 B.C., Nabuchodonosor, king of Babylon, wrote on his slaves' shaved skulls and waited for their hair to grow back, then sent them to his generals. One had to shave the slaves' head to read the message. One may notice the strength of such system: an intercepted message would be detected.

The first real cryptographic systems appeared around 200 B.C. They were mainly tools that made the decyphering very difficult for anyone that did not have the algorithm and the encoding parameters. These systems were encoded either with substitution, mono-alphabetic, poly-alphabetic, homophonic, or polygrams. As technology evolved cryptanalyst's work simplified causing cryptographers to invented more complex methods. The mastering of electricity lead to strong development of telecommunications, literally communication between distant parties. It also resulted in cryptographic automatization using electromechanical systems. The development of computers, enabling quick and repetitive computation, revolutionize the cryptographic field. It have become more and more complex ever since.

The need for secure communication is everywhere today. Though, it is not necessary to have the same security level for home mail and for the red phone between Washington and Moscow. Classical cryptographic systems rely on mathematical conjectures, which are sometimes very complex. Today's algorithms such as PGP or RSA rely on non-proven

mathematical conjectures, thus are potentially breakable. Such algorithm are sufficient tough for personal use.

To have perfectly secure communications, Shannon communication theory showed the need for a *secret* key between parties. Theoretically, classical communications cannot generate a secret between remote parties. One must find another mean to create a secret. During the early 80s, Wiesner, Bennett, and Brassard had the idea to use quantum physics to transmit secret information. Uncertainty is a fundamental property of quantum physics that may be used in a positive manner to build quantum communication protocols. The security level with quantum cryptography may be physically guaranteed up to any desired level making it suitable for military or banking applications.

Quantum communication started growing in 1992 with the first prototype developed by Bennett and Brassard over a 32cm free air link. Since then, many laboratories have worked on quantum cryptography and now this technology has spread to industry.

Since its creation in 1995, the GTL-CNRS Telecom laboratory has studied quantum cryptography, making it a pioneer in the field. Jean-Marc Merolla and Laurent Durrafourg invented a quantum key distribution system that uses a single side band detection scheme (SSB). This thesis focuses on this system and new developments on its security properties. Moreover, it will also introduces a new single side pulse detection scheme (SSP) that inherits the same security properties as the SSB. The use of both system with multiplexing leads to an increase of the secure throughput.

Chapter 1 describes the evolution of classical cryptography systems and how the algorithms are processed. Classical communications are analyzed using Shannon's information theory to define a security criterion for secure communications. The keystone for secure encryption is to have a secure encryption seed. Quantum cryptography may solve this specific problem and enable secret growing between remotes parties.

Chapter 2 explains several quantum key distribution protocols including the classical BB84 protocol and their security strengths and weaknesses. One can then define a security criterion to guarantee the generation of a secret communication key. This section also includes the description of a *strong reference* in a quantum system as a security tool.

The SSB modulation scheme is described in Chapter 3, as well as the SSP system. This section includes the implementation of the BB84 protocol for both systems. Moreover, this specific system implements a *strong reference* which leads to a strong improvement in the security when using a laser source. The security to that of a perfect single photon source. The multiplexing of SSB and SSP is introduced to enhance the secure throughput.

Lastly, Chapter 4 describes the experimental implementation of the SSB principle for quantum key distribution. The system enables long and stable transmission tests. Moreover, an improvement of the system lead to an auto-compensation of the optical path fluctuations. This makes the system robust over the physical variations of the fiber.

Communication methods have drastically evolved since the creation of writing. In ancient times, couriers carried written messages between persons directly. Today, people communicate with satellites or underseao optical fiber. An important use of communications includes confidential data–such as military, banking, or personal information–that cannot be transmitted plainly over a classical channel where everybody would be able to read and copy. In ancient times, privacy was guaranteed with empirical systems. For example, around 600 B.C., Nabuchodonosor, king of Babylon, wrote on his slaves' shaved skulls and waited for their hair to grow back, then sent them to his generals. One had to shave the slaves' head to read the message. One may notice the strength of such system: an intercepted message would be detected.

The first real cryptographic systems appeared around 200 B.C. They were mainly tools that made the decyphering very difficult for anyone that did not have the algorithm and the encoding parameters. These systems were encoded either with substitution, mono-alphabetic, poly-alphabetic, homophonic, or polygrams. As technology evolved cryptanalyst's work simplified causing cryptographers to invented more complex methods. The mastering of electricity lead to strong development of telecommunications, literally communication between distant parties. It also resulted in cryptographic automatization using electromechanical systems. The development of computers, enabling quick and repetitive computation, revolutionize the cryptographic field. It have become more and more complex ever since.

The need for secure communication is everywhere today. Though, it is not necessary to have the same security level for home mail and for the red phone between Washington and Moscow. Classical cryptographic systems rely on mathematical conjectures, which are sometimes very complex. Today's algorithms such as PGP or RSA rely on non-proven mathematical conjectures, thus are potentially breakable. Such algorithm are sufficient tough for personal use.

To have perfectly secure communications, Shannon communication theory showed the need for a *secret* key between parties. Theoretically, classical communications cannot generate a secret between remote parties. One must find another mean to create a secret.

During the early 80s, Wiesner, Bennett, and Brassard had the idea to use quantum physics to transmit secret information. Uncertainty is a fundamental property of quantum physics that may be used in a positive manner to build quantum communication protocols. The security level with quantum cryptography may be physically guaranteed up to any desired level making it suitable for military or banking applications.

Quantum communication started growing in 1992 with the first prototype developed by Bennett and Brassard over a 32cm free air link. Since then, many laboratories have worked on quantum cryptography and now this technology has spread to industry.

Since its creation in 1995, the GTL-CNRS Telecom laboratory has studied quantum cryptography, making it a pioneer in the field. Jean-Marc Merolla and Laurent Durrafourg invented a quantum key distribution system that uses a single side band detection scheme (SSB). This thesis focuses on this system and new developments on its security properties. Moreover, it will also introduces a new single side pulse detection scheme (SSP) that inherits the same security properties as the SSB. The use of both system with multiplexing leads to an increase of the secure throughput.

Chapter 1 describes the evolution of classical cryptography systems and how the algorithms are processed. Classical communications are analyzed using Shannon's information theory to define a security criterion for secure communications. The keystone for secure encryption is to have a secure encryption seed. Quantum cryptography may solve this specific problem and enable secret growing between remotes parties.

Chapter 2 explains several quantum key distribution protocols including the classical BB84 protocol and their security strengths and weaknesses. One can then define a security criterion to guarantee the generation of a secret communication key. This section also includes the description of a *strong reference* in a quantum system as a security tool.

The SSB modulation scheme is described in Chapter 3, as well as the SSP system. This section includes the implementation of the BB84 protocol for both systems. Moreover, this specific system implements a *strong reference* which leads to a strong improvement in the security when using a laser source. The security to that of a perfect single photon source. The multiplexing of SSB and SSP is introduced to enhance the secure throughput.

Lastly, Chapter 4 describes the experimental implementation of the SSB principle for quantum key distribution. The system enables long and stable transmission tests. Moreover, an improvement of the system lead to an auto-compensation of the optical path fluctuations. This makes the system robust over the physical variations of the fiber.

CHAPTER I

CRYPTOGRAPHY AND SECURITY

Transmitting encrypted messages appeared as early as ancient Roman times. The art of war required secret transmission of orders to the battle field. The purpose of secret was to hide the information if the messenger was caught by enemies. Modern uses also require secure transmission means for military, diplomatic, and personal data. Encryption methods have improved over time. Supercomputers and algorithmic improvements allow techniques to break codes that were supposed to be *unbreakable*. For 25 years, a new way of securing information has been developing, born by a marriage with physics and computer science[1]: Quantum cryptography, and specifically quantum key distribution (QKD). The transmission security of QKD relies on physical properties, not on purely mathematical concepts.

This chapter first describes the evolution of cryptography over time. Communicating parties need to share an initial secure key for secrecy. Then, quantum cryptography is introduced as a method for secret key distribution.

1.1 Cryptography and Information Theory

The word cryptography comes from *cryptographia*, a pseudo-Latin word invented during the Middle Ages. It was coined from two Greek roots: the adjective $\kappa\rho\upsilon\pi\tau\grave{o}\varsigma$ (hidden) and the noun $\gamma\rho\alpha\phi\grave{\eta}$ (writing). It was the art of transforming plain messages into number strings. The message transformation procedure has been developed especially since the 14th century. It was called *le nombre* (the "number") [21]. Modern cryptography relies on mathematical encoding techniques, known *classical* cryptography.

Cryptographic techniques were created in an empiric way. It was assumed that without knowledge of the code, it would be impossible to decrypt a message. However, Information

[1]Bennett and Brassard, quantum cryptography inventors, first met October 1979 when they were both swimming in Caribbean Islands. Quantum cryptography is born under the sun!

theory, introduced by Shannon in 1948 [59], specifically quantified the *information content* of a plain message. The notion of secret, or confidentiality, was then rigorously defined by this.

This section explains some basic and more complex cryptographic systems. The role of cryptographic keys for secret transmission between parties is described. Information theory also formalizes the information content of any transmission and its secrecy.

1.1.1 Cryptography and Encryption Keys

Cryptography transforms an understandable plain message, often a written text, into an encoded message, which only parties with a "secret code" are able to decode and understand clearly. The corresponding parties need to define a mean to transform a plain text into an encrypted message and vice versa. Moreover, an eavesdropper that gains access to the encrypted message is not able to easily recover the plain text. Cryptographic systems range from very basic alphabetic substitution to more complex systems based on number theory. Cryptographic applications are designed to ally easy and fast encoding and decoding when the key is known. On the other hand, without knowledge of the key, it is almost impossibility to decode the message.

1.1.1.1 Monoalphabetic Cryptographic Systems

A cryptographic system is defined as a set of all possible plain messages $\mathcal{M}$, encrypted messages $\mathcal{C}$, and encryption keys $\mathcal{K}$. It also includes encryption methods $\mathcal{E}$ and decryption methods $\mathcal{D}$. The symbolic format is the five-uplet $(\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$:

$$\begin{aligned} \mathcal{M} &= \{\text{plain messages } x\} \\ \mathcal{C} &= \{\text{encrypted messages } y\} \\ \mathcal{K} &= \{\text{keys } k\} \\ \mathcal{E} &= \{e_k : \mathcal{M} \to \mathcal{C} | k \in \mathcal{K}\} \\ \mathcal{D} &= \{d_k : \mathcal{C} \to \mathcal{M} | k \in \mathcal{K}\}, \end{aligned}$$

where e_k and d_k are the encryption and decryption functions. This system must meet the following property: for all plain messages x in $\mathcal{M}$ and encryption keys k in $\mathcal{K}$, the encrypted

message $y = e_k(x)$ is in $\mathcal{C}$ and there exists a decryption key k^{-1} in $\mathcal{K}$ that allows decryption of y:

$$\forall x \in \mathcal{M}, \forall k \in \mathcal{K}, \exists k^{-1} \in \mathcal{K} | d_{k^{-1}}(e_k(x)) = x. \quad (1)$$

A first set of basic cryptographic systems includes monoalphabetic systems. The most simple of them are substitutions. Each letter is changed into its position in the alphabet, see Figure 1. Each letter is always encoded into the same number. The symbolic definition of substitution for a message of length n_0 is the set $(\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$:

$$\begin{aligned}
\mathcal{M} &= \{a, b, c, d, ..., z\}^{n_0} \\
\mathcal{C} &= \{0, 1, 2, ..., 25\}^{n_0} \\
\mathcal{K} &= \{0\} \\
\mathcal{E} &= \{e_0 : a \mapsto 0, b \mapsto 1, ..., z \mapsto 25\} \\
\mathcal{D} &= \{d_0 : 0 \mapsto a, 1 \mapsto b, ..., 25 \mapsto z\}.
\end{aligned}$$

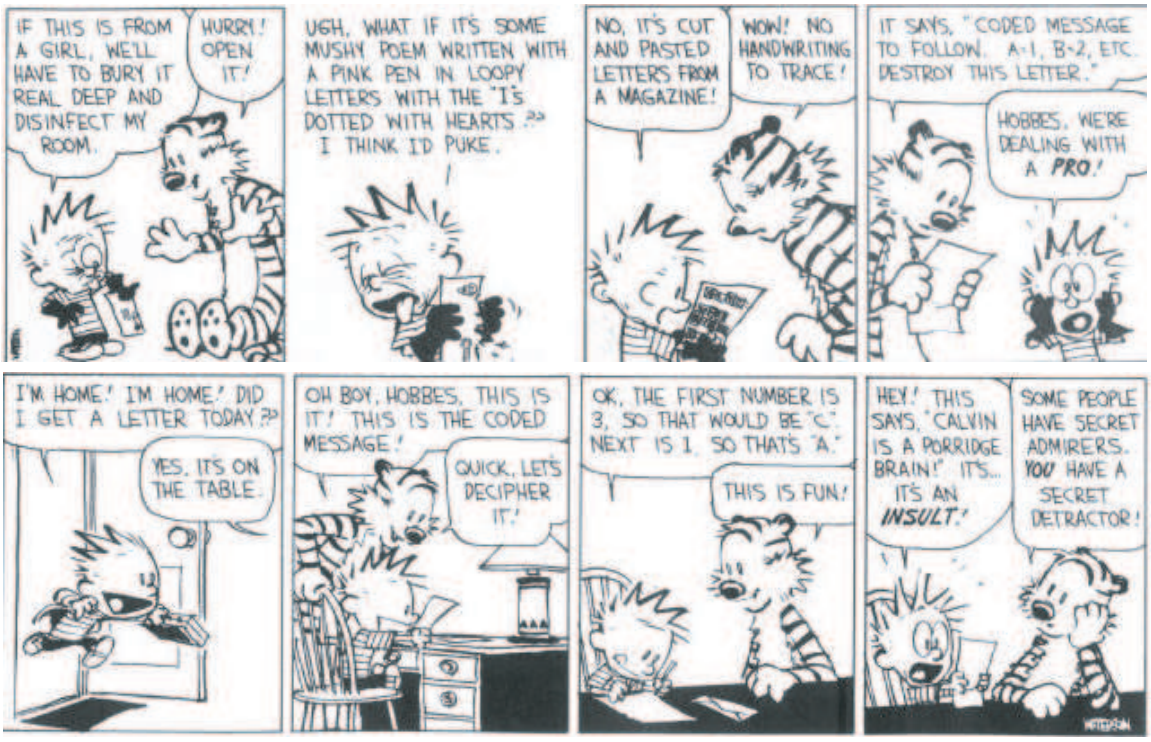


Figure 1: Encryption by Calvin and Hobbes [70]. The method used is a very basic alphabetic substitution. Homicidal Psycho Jungle Cat copyright ©1994 by Bill Watterson.

Only one key is used in this cryptographic system. Thus, there is only one encryption function e_0 and only one decryption function d_0. An eavesdropper tapping in the transmitted signal and knowing the encryption technique could decrypt the message. This weakness is due to the single possible encryption key, i.e., $\text{card}\{\mathcal{K}\} = 1$. This is an example of Kerckhoffs' principle [43], which states that secret should be included in the encryption and decryption key, and not based on secrecy of the encoding technique, which cannot be reasonably guaranteed.

More complex cryptographic systems are monoalphabetic systems. The encryption and decryption shift the letter position in the alphabet. Thus, for a given shift n, the encryption function maps a to n, b to $n+1$, etc... The whole cryptographic system is then for an n_0 length message:

$$\begin{aligned}
\mathcal{M} &= \{a, b, c, d, ..., z\}^{n_0} \\
\mathcal{C} &= \{0, 1, 2, ..., 25\}^{n_0} \\
\mathcal{K} &= \{0, 1, 2, ..., 25\} \\
\mathcal{E} &= \{e_n : a \mapsto n, b \mapsto n+1, ..., z \mapsto n+25\} \\
\mathcal{D} &= \{d_n : n \mapsto a, n+1 \mapsto b, ..., n+25 \mapsto z\},
\end{aligned}$$

where the corresponding number addition is always modulo 26. In this system, the encryption key is the shift value n. There are thus, 26 possible keys, $\text{card}\{\mathcal{K}\} = 26$.

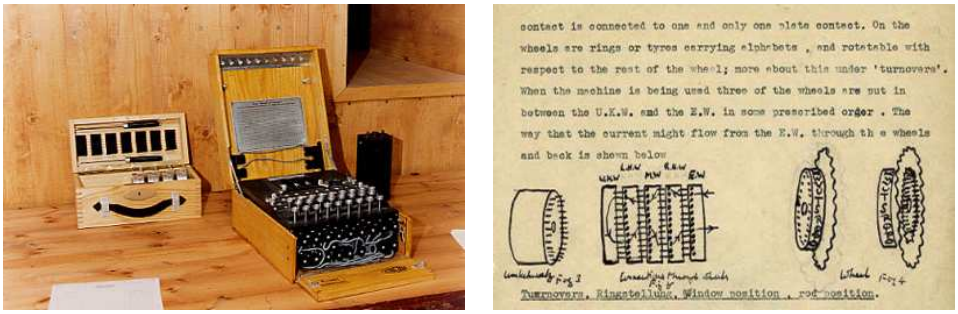
Finally, the most general substitution is based on assigning randomly a value to a letter, then constructing a substitution table from this. The number of possible keys is then the number of possible permutations of the set $\{0, 1, ..., 25\}$, $\text{card}\{\mathcal{K}\} = 26! \approx 4 \cdot 10^{26}$ possible keys. Although this number looks very large, the major weakness of this system is the single encoding for each letter. When an eavesdropper knows the initial language, a statistical attack on an encrypted message can recover the substitution table, and thus decrypt the message [58].

A complex cryptographic system must encrypt a specific letter as a function of the surrounding characters, which is as a function of the context. As basic substitutions are not enough, polyalphabetic systems need to be developed.

1.1.1.2 Alphabetic Polysubstitution

Following Kerckhoffs' principle, one needs to build a system where the encryption key number is very large, i.e., card$\{\mathcal{K}\} \gg 1$, and where the knowledge of one encrypted message does not allow direct attacks. A "brute force" attack, which is to try all possible keys, should not be possible directly and practical. Polysubstitution alphabetic systems have been developed to increase the number of possible encryption keys.

The Enigma machine is an example of polysubstitution alphabetic system. It was actively used by Germans during World War II. It scrambles plain text letters with an electromechanical apparatus, see Figure 2. Initial text is entered through a keyboard with keys scrambled by a wiring panel that switches letters two by two. Then, three moving rotors scramble the electrical signal again. It is reflected again through the rotors and the wiring panel. Finally the letters appear on a light bulb array, see Figure 2(b). A mechanical system shifts the rotors' position after every encoded letter. Each letter match depends on both the initial key and its position in the message. Thus, the encryption key is the rotors' initial position and the wiring of the connection panel.



(a) The Enigma machine. (b) Turing's note on Enigma [67].

Figure 2: The Enigma machine.

The number of possible encryption keys for Enigma was above 10^{16}, making brute force attacks impossible. With this large number of possibilities, and without computer technology in 1940, the Germans were fully confident in their cryptographic apparatus[2]. Though, Benchley Park's English cryptanalysts tasked specifically to the study of this

[2]A brute force attack would take only a few minutes with today's computer.

machine, managed to crack the code. They used its weaknesses, such as its symmetric characteristics. The English were able, thanks to Turing [67], to decrypt German messages in an efficient ways.

1.1.1.3 Computational Complexity, Easy and Complex Codes

The difficulty to attack a system may be evaluated by its *computational complexity*. An algorithm complexity is the number of required steps as a function of the input size, i.e., the length of the message to study. For example, searching a magnetic tape is of linear complexity, as one need to read the whole tape once. A dictionary search is logarithmic, as one need to check the word in the middle of the book, and then proceed to a search in a "half-size dictionary". This is also known as "divide and conquer". Simple problems are those of polynomial complexity, and complex problems are of exponential complexity[3].

Since the 1950s, computing power has drastically increased. As result, new encryption methods have been developed. Mathematical properties based on number theory are useful tools for cryptography, and its counterpart, cryptanalysis. Computers allow long and repetitive calculation to be done efficiently. The limiting factor is then the required time for an exhaustive computer search. One solution to overcome the effectiveness of increasing computing power is to increase the system size and the key size, thus increasing the number of possible encryption and decryption keys.

1.1.1.4 Symmetric Algorithm: The AES code

A symmetric encryption scheme is an algorithm where encryption and decryption are the same operations. One of them is the AES code, also known as "Rijndael"[4] [20]. It was developed by two Belgian cryptographers, Daemen and Rijmen. Initially defined as an encryption standard by the US government and adopted November 2001 by the National Institute of Standards (NIST), this method is today widely used.

[3] One could say that an easy problem could be solved by the computing power of your younger sister and a complex problem requires an NSA Cray X1™.

[4] If you're Dutch, Flemish, Indonesian, Surinamer or South-African, it's pronounced like you think it should be. Otherwise, you could pronounce it like "Reign Dahl", "Rain Doll", "Rhine Dahl". I'm not picky. As long as you make it sound different from "Region Deal".

The AES algorithm is a network of substitutions and permutations. It is easy to build, fast when implemented in software or hardware, and requires low amount of memory. It is a block sequential code where different basic operation steps are processed, see Figure 3. The key $\oplus$ is a bitwise XOR between the key and the text, e.g., $66 \oplus fa \mapsto 9c$. The "S-Box" step is a non-linear process that uses a matching table, between plain bytes and encrypted bytes, e.g., $9c \mapsto a2$. The line shift is processed by shifting lines by two bytes for the second line, three bytes for the third line, and six bytes for the last line. The column scrambling is represented by a matrix product of m_{ij} elements in the Galois field $GF(2^8)$ with one column[5]. These operations are repeated nine times and use a different key for each pass. Keys are generated from the initial key by multiplication and permutation in the Galois field.

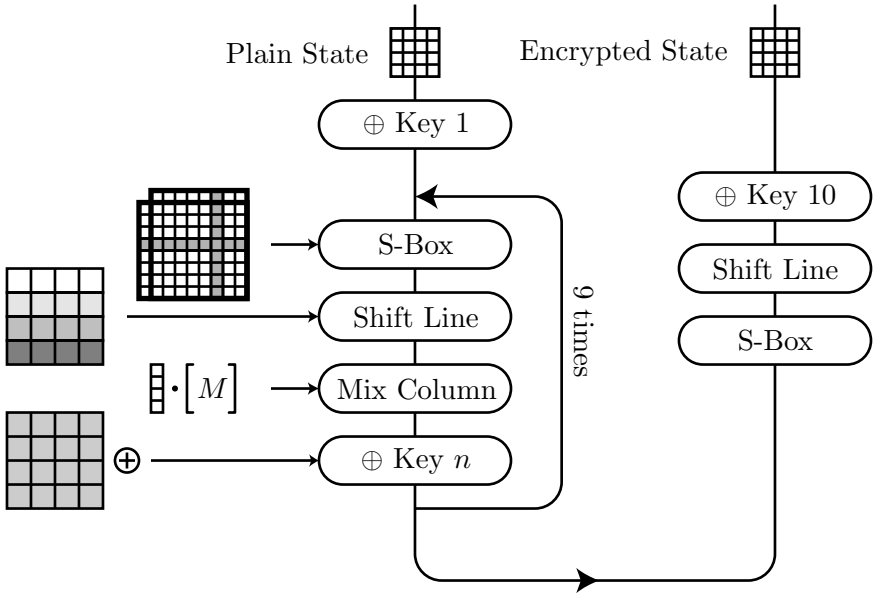


Figure 3: AES code scheme.

There is today no known successful attack on the AES algorithm. Its security has been judged efficient enough by US government to use as a TOP SECRET level encryption method. Even though some cryptanalysts worry about AES security and its mathematical structure, it is much more complex than many block cryptography algorithms. In September 2002, Courtois and Pieprzyk [18] announced a thrilling attack on AES which

[5]A multiplication description in a Galois field may be found in [29].

reveals a potential weakness in the algorithm. Although it requires computing power far more advanced than is available today, the needed technology may be available in a near future. Moreover, some cryptographers criticize mathematical grounds of this paper, and the calculations specifically.

In all previous examples, the emitter and the receiver have access to an encryption and a decryption key respectively, on which they agree before the transmission. These are called secret key systems. The keys have to remain secret to guarantee the secrecy of the transmission. This is where the paradox lies: one must share an initial secret before having a secret transmission. Though, it is possible to implement encryption algorithms that are today unbreakable.

1.1.2 Classical Information and Security

Information theory introduced by Shannon in 1948 [59] defines the information bit in a digital communication. One can then calculate the amount of information per transmitted symbol. In 1949 Shannon worked also with cryptanalysts to publish an application of this theory[6] towards the formalism of secret communication information [60].

This section presents how information theory describes cryptographic systems and links security to encryption keys. It shows that secrecy requires secret encryption keys.

1.1.2.1 Cryptographic System and Perfect Secrecy

Shannon showed that any cryptosystem may be modeled as Figure 4. The plain message x is encrypted into the cryptogram $y = e_{k_1}(x)$. The message is found back by decryption, $x = d_{k_2}(y) = d_{k_2}(e_{k_1}(x))$. In order to make the system solvable, we should consider that *the encryption/decryption system is known by any eavesdropper*, i.e., he/she knows all encryption e_k and decryption d_k functions, as well as the probability distribution for the key k within $\mathcal{K}$. The assumption is part of the Kerckhoffs' rules [43].

The "theoretical security" of a cryptosystem may be considered when an enemy is assured to have access to unlimited time and computing power. A cryptosystem is considered

[6]The content of this paper published in 1949 appear in a confidential report dated September 1st, 1946 and declassified since then.

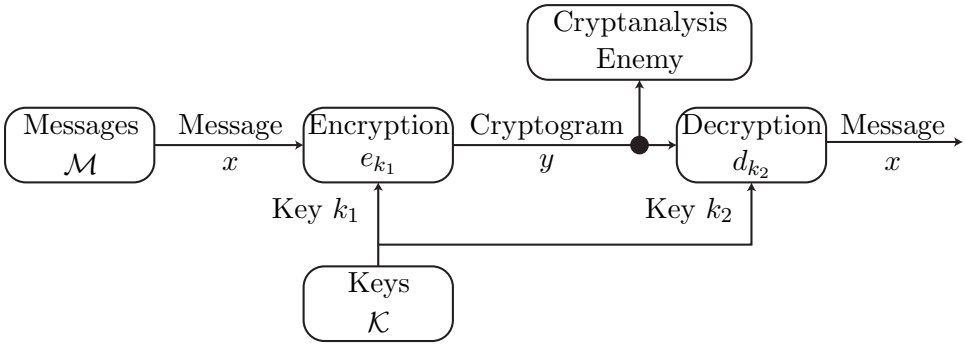


Figure 4: Schematic of a cryptosystem.

to have perfect secrecy when the *a posteriori* probability to know the plain text x when knowing the encrypted message y is the same as the *a priori* probability to know the text x:

$$\forall x \in \mathcal{M}, y \in \mathcal{C}, \text{Prob}(x/y) = \text{Prob}(x). \tag{2}$$

Shannon shows that to achieve perfect secrecy, it requires the amount of possible keys to be at least as large as the amount of possible messages [60], i.e.,

$$\text{card}(\mathcal{K}) \geq \text{card}(\mathcal{M}). \tag{3}$$

1.1.2.2 One Time Pad Encryption Technique

One example of such system presenting as many possible messages, as many possible keys is the one-time pad encryption scheme. It meets perfect secrecy requirement of Equation (2). A random encryption key, as lengthy as the message itself, is used once and then changed for each following transmission. Encryption is made by an XOR operation between the key and the plain message. The decryption method is the exact same operation; an XOR of the encrypted text with the key gives the plain message back. This technique initially described by Vernam [68] at the beginning of the twentieth century guarantees that an eavesdropper reading the encrypted message derive absolutely no information on the plain message using the encrypted message.

An example of one time pad use is the communication between Fidel Castro and Che Guevara, see Figure 5. The initial text is transformed through a mapping table to give the message M. The message is added modulo 10 to the encryption key k, known only by

Che Guevara and Fidel Castro, to give the cryptogram y that may then be transmitted in a public manner to Castro by radio signal for example. The same operation on y allows recovery of the plain message x. Security of such a system relies on the private sharing of the secret key used for both encryption and decryption.

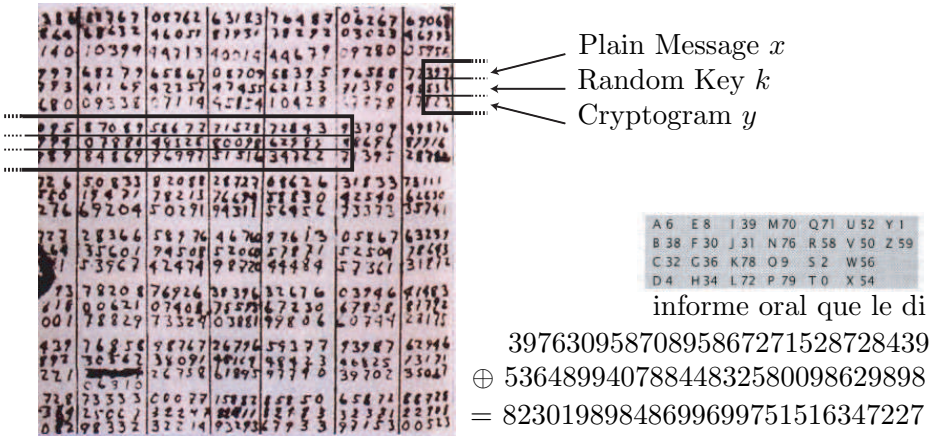


Figure 5: One Time Pad scheme example between Che Guevara et Fidel Castro. Note found on Che Guevara during his arrestation by Bolivian military. The Spanish text says: *"...informe oral que le di..."* meaning: "...the oral report I gave him..."

1.1.2.3 Authentication and Identification

All cryptographic applications work when the message has not been modified or replaced. A key must be transmitted from the emitter to the receiver and must fulfill two conditions. The first condition is to make sure that the key has not been modified during transmission -a process called authentication- to guarantee message integrity. The emitter and receiver, usually called Alice and Bob[7], must also trust the other party, this is called *identification*. They can then check the origin of a message anytime.

When identification is used, it is then impossible for an eavesdropper to perform a man-in-the-middle attack which consists in spoofing both Alice and Bob by pretending to be Alice to Bob and to be Bob to Alice.

Identification may be performed first by considering that Alice and Bob share a common

[7]Schneier introduced a table of dramatis personae headed by Alice and Bob [58]. Others include Carol (a participant in three- and four-party protocols), Dave (a participant in four-party protocols), Eve (an eavesdropper), Mallory (a malicious active attacker), Trent (a trusted arbitrator), Walter (a warden), Peggy (a prover) and Victor (a verifier). These names for roles are either already standard or, given the wide popularity of the book, may be expected to quickly become so.

secret: a *password* that they exchange at the beginning of each communication. Needham and Guy showed that Alice and Bob do not need to know the other's actual password, but that they only need to be able to differentiate a valid password from an invalid one. Then, only results from hashing functions of passwords are compared. This prevents an eavesdropper to recover the initial password.

Authentication may also be implemented with hashing functions. A initial secret key is used to sign a document, validating the message non-alteration during transmission.

All previous processes require an initial secret to be shared between Alice and Bob. Its length is to be the logarithm of the message length. For example, if Alice and Bob share a secret of length n_0, they may be able to *sign* a message of lengths no greater than e^{n_0} to guarantee integrity of the message [58].

1.1.3 From Mathematical Strength to Physics Power

Encryption and decryption with prefect secrecy is achievable by using the one time pad scheme. Though, one must transmit the key from Alice to Bob in a secure fashion first.

Another class of algorithms was developed, the *public key* cryptosystems. These allow one-way secure transmission over a public channel guaranteed on mathematical properties. The typical scheme of such system is to publish a bit string A, the public key, that allows one to encrypt a message, such that only the authorized receiver may decrypt the message with the corresponding private key B, with the private key B being only known by the receiver. In the same fashion, a public key A may allow one to decrypt messages that only the legitimate sender can encrypt with the private key B.

The security of such system relies on mathematical properties or unproven conjectures. One should note that in case of a conjecture, the security of the communication is not 100% guaranteed as a genius may have already found a way to disprove this conjecture, but has not yet published it.

1.1.3.1 Public Key System: RSA Code

An example of such system is the globally used RSA code, named from its three inventor's name Ron Rivest, Adi Shamir, and Leonard Adleman [56]. It is a symmetric scheme, i.e.,

encryption e_k and decryption d_k functions are the same ones. Let us assume an integer n to be the product of two large prime numbers p and q. The crypto system may be described by:

$$\begin{aligned}
\mathcal{M} &= \mathbb{Z}/n\mathbb{Z} \text{ and } \mathcal{C} = \mathbb{Z}/n\mathbb{Z} \\
\mathcal{K} &= \{e \text{ invertible in } \mathbb{Z}/\varphi(n)\mathbb{Z}\} \\
\mathcal{E} &= \{e_k : m \mapsto m^k \text{ (modulo } n)\} \\
\mathcal{D} &= \{d_k : c \mapsto c^k \text{ (modulo } n)\}
\end{aligned}$$

where $\mathbb{Z}/n\mathbb{Z}$ is the group of integers modulo n and $\varphi(n)$ is the Euler indicator [29]. Messages are described modulo n and encryption and decryption functions are proceed with powers modulo n. A decryption key $k \in \mathcal{K}$ is associated to a decryption key $d \in \mathcal{K}$ which is the inverse[8] of $e \in \mathcal{K}$ in $\mathbb{Z}/\varphi(n)\mathbb{Z}$. The secret pair (e, d) allows the recovery of encrypted messages [29].

If an eavesdropper intercepts the public key (n, e), and the encrypted message y, she cannot directly access the number d that is kept secret. Eve must compute p and q from n in order to compute $\varphi(n)$, and then d from e. There exists no known algorithm allowing one to factorize the product of two large prime numbers in logarithmic complexity using a classical computer[9]. It is also not yet proven that factorizing n is the best way to crack RSA. In any case, one can consider this algorithm to be secure enough for the present, but encrypted messages may be recorded now and decrypted in the future when a new technique will be available.

This algorithm, as well as all public key algorithms, has a strong weakness; it is slow -much slower than its symmetric counterpart. For large data applications, public key algorithms can not be used economically. A solution is to use hybrid systems. First encryption keys are exchanged with an asymmetric public key algorithm, and second a symmetric algorithm is used for the data encryption. The well known Pretty Good Privacy[10] (PGP)

[8] An algorithm for finding an inverse modulo n may be found in Schneier [58].

[9] We should say: we do not know today such a classical algorithm. Though, Peter Shor found an efficient algorithm to factorize a product of two primes on a quantum computer [61].

[10] The name "Pretty Good Privacy" was inspired by the name of the grocery store featured in radio host Garrison Keillor's fictional town, Lake Wobegon. The grocery was "Ralph's Pretty Good Grocery".

originally designed and developed by Phil Zimmermann in 1991, widely used to encrypt emails, is built on this scheme.

1.1.3.2 Brute Force or Exhaustive Attack

Confusion may occur with the word "attack" from its different definitions. For a cryptographer, an attack is any process that allows one to find the key faster than an exhaustive attack, even if completely unpractical. For an engineer, an attack is something practical now, or that may be at least implemented in a near future. For example, an algorithm could be a possible attack for a cryptographer, as it lowers the complexity of the algorithm, but still not an engineer.

A *brute force attack* is an exhaustive trial of all possible keys on a cryptosystem. It is brutal in a sense that it requires no "thinking", only systematic trials of every possible key. Such an attack has become possible by using distributed resources. RSA labs launched a challenge to find the encryption key of a short encrypted message. The distributed.net team found the 56 bit key on October 19th, 1997 at 1:25pm UTC.

One must then strongly secure the key transmission, and one should be able to change this key quite often. The previous described techniques rely on mathematical conjectures where encryption algorithm complexity guarantees the transmission security. Moreover these systems may be retroactively attacked. New methods have to be found to have secure communication, and to guarantee absolute security. Using one time pad encryption scheme, one can guarantee the security of key transmission.

1.2 QKD: From the BB84 Protocol to strong reference protocol

Quantum physics may look counter-intuitive in a macroscopic world, and especially its uncertainty principle. Though, as its laws may not be broken, it is possible to use them to guarantee transmission absolute security. Quantum physics allows the development of a new field, quantum cryptography, where security relies on *physical* properties and laws.

Quantum cryptography was born around 1970 from an idea of Wiesner [73], and from Bennett and Brassard in 1984 [7]. The following quantum principles sustain quantum

cryptography:

1. It is impossible to perfectly copy an unknown quantum state. This principle is also known as the non-cloning theorem [74].

2. Any measurement disturbs the system.

3. Measurements are probabilistic.

The first property illustrates a fundamental principle in quantum physics: *uncertainty*. If one desires to proceed to two simultaneous non orthogonal measurements on a quantum particle, the results will remain uncertain. The second property shows the sensitive character of quantum particles. Uncertainty in quantum physics allows one to build quantum communication protocols. These two properties allow one to check if an eavesdropper is tapping the signal, thus also disturbing the quantum signal between Alice and Bob.

Historically, the first described protocol, the BB84 [7], uses orthogonal quantum measurement to construct a key sharing between Alice and Bob. Then, protocols have evolved and use more complex measurements, the POVM described in Section 1.2.2. Finally, quantum information processing allows one to build more complex schemes using EPR states, squeezed states, or continuous quantum variables.

This section describes the main protocols evolution. Different quantum state preparations and measurements can be used to build a secret communication scheme that guarantees the confidentiality of such communications.

1.2.1 Orthogonal Quantum Measurement and BB84 Protocol

1.2.1.1 Quantum States and Bra-ket

Quantum cryptography uses quantum particles to carry information, more specifically the value of a state variable. Such a variable may be modeled in a Hermitian space E. One specific state may be described with a state vector called *ket* and written $|\psi\rangle \in E$. This space E comes with a scalar product $\langle\varphi|\psi\rangle$ where $|\psi\rangle$ belongs to E and $\langle\varphi|$ belongs to E^*, the dual space of E. $\langle\varphi| \in E^*$ is called *bra*, and its scalar product is called *braket*. The bra-ket satisfies the properties of a Hermitian scalar product, i.e., $\forall\lambda_1, \lambda_2 \in \mathbb{C}$ and

$\forall \varphi_1, \varphi_2, \psi_1, \psi_2, \varphi, \psi \in E$:

$$\langle \lambda_1 \varphi_1 + \lambda_2 \varphi_2 | \psi \rangle = \lambda_1^* \langle \varphi_1 | \psi \rangle + \lambda_2^* \langle \varphi_2 | \psi \rangle \text{ and}$$

$$\langle \varphi | \lambda_1 \psi_1 + \lambda_2 \psi_2 \rangle = \lambda_1 \langle \varphi | \psi_1 \rangle + \lambda_2 \langle \varphi | \psi_2 \rangle \qquad \text{(sesquilinearity)}$$

$$\langle \psi | \psi \rangle \in \mathbb{R}^+ \qquad \text{(positivity)}$$

$$(\langle \psi | \psi \rangle = 0) \Rightarrow (|\psi\rangle = |0\rangle) \qquad \text{(definite)}$$

Hermitian spaces considered for quantum cryptography are usually two dimensional. The first quantum key distribution implementation [6] used photon polarization as the quantum variable. It considers two rectilinear, orthogonal, and same amplitude photon polarizations, $|u\rangle$ and $|v\rangle$, that generates an orthonormal basis B. For all photon polarization states $|\psi\rangle$ of same amplitude as state $|u\rangle$, one can find $a, b \in \mathbb{C}$ such as this state is a linear combination of basis B vectors:

$$|\psi\rangle = a|u\rangle + b|v\rangle. \tag{4}$$

This decomposition fulfills the following condition for unit photon state $|\psi\rangle$:

$$\| \, |\psi\rangle \, \|^2 = |a|^2 + |b|^2 = 1. \tag{5}$$

1.2.1.2 Quantum Variable or qubit

It is possible to define a *qubit*[11] (or quantum bit) used in quantum information processing. Contrary to regular bits that can have only two possible value (often written `0` and `1`), a qubit may have a continuum of values of form $a|0\rangle + b|1\rangle$ where a and b satisfy Equation (5). A qubit, or state $|\psi\rangle = a|u\rangle + b|v\rangle$, may be represented by a point (θ, ϕ) on the unit sphere, called Bloch sphere, see Figure 6. Angles θ and ϕ are defined by:

$$a = \cos(\theta/2), \tag{6}$$

$$b = e^{i\phi} \sin(\theta/2), \tag{7}$$

where a is a real, that may be obtained by multiplying $|\psi\rangle$ by a phase factor, which is not observable. Then $|\psi\rangle$ is represented with a unitary vector $(\cos\phi \sin\theta, \sin\phi \sin\theta, \cos\theta)$ called *Bloch vector*.

[11] A qubit is not to be confused with a cubit, which is an ancient measure of length.

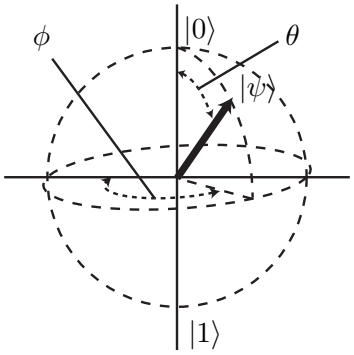


Figure 6: Qubit or state vector $|\psi\rangle$ representation on the Bloch sphere.

When a quantum state $|\psi\rangle$ is prepared, there are two ways to measure the value of this variable. The first method, introduced by von Neumann [69], is the standard quantum measure, also called orthogonal measure or Neumann measure. The second way, the measure with POVM, is described in Section 1.2.2.

1.2.1.3 Orthogonal Quantum Measurement

The measure of a *measureable* physical length $\mathcal{P}$, may be described with a Hermitian operator P of E, called *measurement*. This measurement is an autoadjoint endomorphism [29], that satisfies $P^* = P$, its eigenvalues λ_n are real, and its eigenvector set $\{|u_n\rangle\}_n$ spans an orthonormal basis of E. Assuming P_n to be the orthogonal projection on vector $|u_n\rangle$, P_n and P may be expressed as:

$$P_n = |u_n\rangle\langle u_n| \qquad \text{and} \tag{8}$$

$$P = \sum_n P_n = \sum_n |u_n\rangle\langle u_n|. \tag{9}$$

When a measurement P is applied to a vector $|\psi\rangle$, quantum mechanics imposes that the outcome of the measurement is one of the eigenvectors $|u_n\rangle$ with a probability p_n:

$$p_n = \|\langle u_n|\psi\rangle\|^2 = \langle\psi|u_n\rangle\langle u_n|\psi\rangle = \langle\psi|P_n|\psi\rangle. \tag{10}$$

One can note that the probabilities sum is 1, that is:

$$\sum_n p_n = \sum_n \langle\psi|P_n|\psi\rangle = \langle\psi|\sum_n P_n|\psi\rangle = \langle\psi|P|\psi\rangle = \|P|\psi\rangle\|^2 = 1, \tag{11}$$

because P is Hermitian, thus, it conserves norms on E. The initial state $|\psi\rangle$ becomes with probability p_n the state:

$$\frac{1}{\sqrt{p_n}} P_n |\psi\rangle. \tag{12}$$

Any measurement P projects any state $|\psi\rangle$ on one of its eigenstates $|u_n\rangle$ with a probability $1/\sqrt{p_n}$. Contrary to the classical case, measurement is probabilistic. Unless the system was previously in one of the eigenstates of the observable, the system is modified by measurements.

1.2.1.4 The BB84 Protocol

The first quantum cryptography protocol introduced by Bennett and Brassard in 1984 uses orthogonal projections and Neumann measurement, hence its acronym BB84 [7]. Initially described with photon polarization, this protocol may be used with any quantum state variable.

Alice and Bob initially use four states $|u_1\rangle, |u_2\rangle, |v_1\rangle, |v_2\rangle$, from a two dimension Hermitian space, satisfying:

$$\langle u_1|u_2\rangle = \langle v_1|v_2\rangle = 0, \tag{13}$$

$$\langle u_1|v_1\rangle = \langle u_1|v_2\rangle = \langle u_2|v_1\rangle = \langle u_2|v_2\rangle = \frac{1}{2}. \tag{14}$$

$B_U = \{|u_0\rangle, |u_1\rangle\}$ and $B_V = \{|v_0\rangle, |v_1\rangle\}$ are orthonormal bases of E. Moreover, Equation (14) shows that $|u_0\rangle$ and $|u_1\rangle$ belong to the bisector plan of $[|u_0\rangle, |u_1\rangle]$. One possible solution is:

$$|v_0\rangle = \frac{|u_0\rangle + |u_1\rangle}{\sqrt{2}} \text{ and } |v_1\rangle = \frac{|u_0\rangle - |u_1\rangle}{\sqrt{2}}. \tag{15}$$

The four BB84 protocol states may be represented on the Bloch sphere, see Figure 7.

As $|u_0\rangle$ and $|u_1\rangle$ are orthogonal, it is possible to build a measurement M_U that gives a deterministic outcome for these two states, see Figure 8(a). In the same manner, it is possible to build M_V in order to separate $|v_0\rangle$ and $|v_1\rangle$, see Figure 8(b). One can then note that measurement M_U applied to $|v_0\rangle$ or $|v_1\rangle$ gives the outcome $|u_0\rangle$ or $|u_1\rangle$ with probability $1/2$.

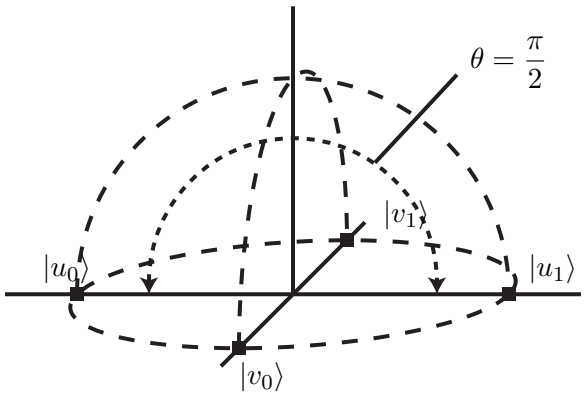
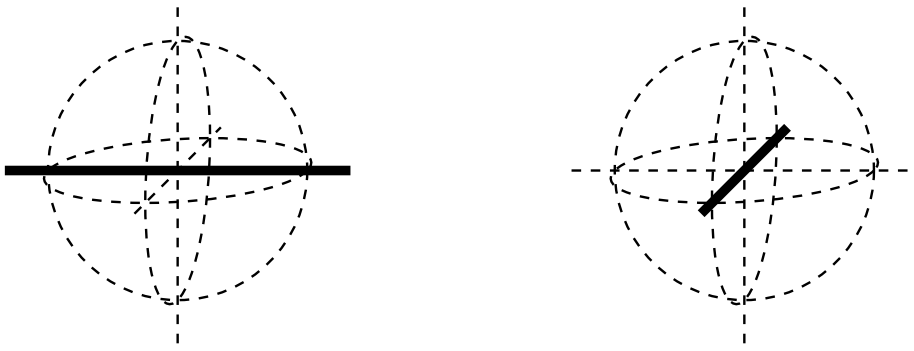


Figure 7: The four states associated with BB84 protocol.



(a) Measurement M_U, projection on $|u_0\rangle$ and $|u_1\rangle$.

(b) Measurement M_V, projection on $|v_0\rangle$ and $|v_1\rangle$.

Figure 8: Orthogonal Measurement Representation of M_U et M_V built from initial vectors $|u_0\rangle, |u_1\rangle, |v_0\rangle, |v_1\rangle$.

The probability to detect a state $|\psi\rangle$ on an eigenstate $|\varphi\rangle$ depends on the angle θ between the two states. The corresponding probability is $p = \cos^2\theta$.

To build a communication protocol, Alice and Bob assign bit value `0` to states $|u_0\rangle$ and $|v_0\rangle$ and bit value `1` to states $|u_1\rangle$ and $|v_1\rangle$. When Bob applies the proper measurement on a quantum state $|\psi\rangle$, i.e., the one built from the state $|\psi\rangle$, he can determine the sent state exactly. *A contrario*, if he applies the wrong measurement, the outcome is random because of the 1/2 probability for each.

The BB84 protocol uses the following steps:

1. Alice randomly prepares a state $|\psi\rangle$ among the four possible values and sends it to Bob. The *random* character of basis choice is here fundamental. The basis choice is a random, independent, and equiprobable process.

2. Bob receives the state $|\psi\rangle$ and applies a measurement M_U or M_V chosen randomly, i.e., he makes a projection on one of the bases U or V.

3. After the measurement is performed, Bob reveals to Alice on an authenticated public channel the bases he used.

4. Alice and Bob conserve only bits corresponding to states prepared and measured in the same bases.

The whole process, with all possible states and measurements, is summarized in Table 1. Finally, Alice and Bob share a random bit string that may be used as a seed for an encryption key and more complex classical cryptography algorithms.

Table 1: All possible BB84 protocol prepared states and measurements.

Bit	`0`		`1`		`0`		`1`	
Base	U		U		V		V	
Alice State	$\|u_0\rangle$		$\|u_1\rangle$		$\|v_0\rangle$		$\|v_1\rangle$	
Bob Measurement	M_U	M_V	M_U	M_V	M_U	M_V	M_U	M_V
Outcome $M\|\psi\rangle$	$\|u_0\rangle$	$\frac{\|u_0\rangle+\|u_1\rangle}{2}$	$\|u_1\rangle$	$\frac{\|u_0\rangle+\|u_1\rangle}{2}$	$\frac{\|u_0\rangle+\|u_1\rangle}{2}$	$\|v_0\rangle$	$\frac{\|u_0\rangle+\|u_1\rangle}{2}$	$\|v_1\rangle$
Same Basis	Yes	No	Yes	No	No	Yes	No	Yes
Shared Bit	`0`		`1`			`0`		`1`

1.2.1.5 The B92 Protocol

Charles Bennett showed in 1992 that a quantum key distribution protocol may be built with only two non orthogonal states using orthogonal measurements, called the B92 protocol [5].

Two non orthogonal states $|u\rangle$ and $|v\rangle$ are associated with two measurements $M_{\bar{u}}$ and $M_{\bar{v}}$ which are orthogonal to $|u\rangle$ and $|v\rangle$ respectively Then, when these measurements are applied to initial states:

$$M_{\bar{u}}|u\rangle = 0 \text{ and } M_{\bar{u}}|v\rangle > 0 \tag{16}$$

$$M_{\bar{v}}|v\rangle = 0 \text{ and } M_{\bar{v}}|u\rangle > 0. \tag{17}$$

Bob randomly chooses one of either measurement. When he has a non-zero outcome, he can recover the sent state.

This protocol may be explained with positive operator valued measurements (POVM) as described below.

1.2.2 POVM Measurement and B92 protocol

1.2.2.1 The POVM or non-Orthogonal Measurement

The second way to perform a quantum measurement is with *Positive Operator Valued Measurement* (POVM) [10]. Assume two non orthogonal states $|u\rangle$ and $|v\rangle$, such that $\langle u|v\rangle = \cos\theta \neq 0$. The state $|v\rangle$ may be decomposed as:

$$|v\rangle = \cos\theta|u\rangle + \sin\theta|\bar{u}\rangle, \tag{18}$$

where $|\bar{u}\rangle$ is the orthogonal vector to $|\bar{u}\rangle$ that satisfies Equation (18).

The POVM may be described with a series of three non negative operators:

$$P_{\bar{u}} = \frac{\mathbb{1} - |u\rangle\langle u|}{1 + \langle u|v\rangle} \tag{19}$$

$$P_{\bar{v}} = \frac{\mathbb{1} - |v\rangle\langle v|}{1 + \langle u|v\rangle} \tag{20}$$

$$P_? = \mathbb{1} - P_{\bar{u}} - P_{\bar{u}} \tag{21}$$

where $P_{\bar{u}}$ and $P_{\bar{v}}$ are projectors on subspaces orthogonal to $|u\rangle$ and $|v\rangle$ respectively.

This POVM may be decomposed by first building the operators $P_{\bar{u}}$ and $P_{\bar{v}}$ to void states $|u\rangle$ and $|v\rangle$. The operator $P_?$ is then added for the sum to equal $\mathbb{1}$, the identity operator.

The probability to detect $P_{|\bar{u}\rangle}|v\rangle$ and $P_{|\bar{v}\rangle}|u\rangle$, and the third outcome $P_?$ are respectively:

$$\begin{aligned} p_{|\bar{u}\rangle} &= \| P_{|\bar{u}\rangle}|v\rangle \| = \langle v|P_{\bar{u}}P_{\bar{u}}|v\rangle = \langle v|P_{\bar{u}}|v\rangle \\ &= \frac{\langle v|(\mathbb{1} - |u\rangle\langle u|)|v\rangle}{1+\cos\theta} = \frac{1-\cos^2\theta}{1+\cos\theta} = 1-\cos\theta \qquad (22) \\ p_{|\bar{v}\rangle} &= \langle u|P_{\bar{v}}|u\rangle = \frac{1-\cos^2\theta}{1+\cos\theta} = 1-\cos\theta \qquad (23) \\ p_? &= \langle v|P_?|v\rangle \\ &= \frac{\langle v|(-\mathbb{1} + |u\rangle\langle v| + |u\rangle\langle u| + |v\rangle\langle v|)|v\rangle}{1+\cos\theta} = \cos\theta \qquad (24) \end{aligned}$$

Then, one can observe that $p_{|\bar{u}\rangle} + p_? = 1$ and $p_{|\bar{v}\rangle} + p_? = 1$

The probability to have a positive value detection $p_{|\bar{u}\rangle}$ or $p_{|\bar{u}\rangle}$ is not 1, the result is not always conclusive. A POVM allows one to know with a probability $0 < p < 1$ if the state is not colinear to $|u\rangle$. Though, when the outcome is null, it is impossible to conclude if the detected state was $|u\rangle$ or $|v\rangle$.

The non orthogonal measure with POVM allows knowing from time to time the state of an incoming state. Quantum Key Distribution Protocols may be built using orthogonal measurements like the BB84, but also non-orthogonal states as done in the B92.

1.2.2.2 The B92 Protocol

Two non orthogonal states are enough to build a QKD protocol. B92 protocol, initially described with orthogonal measurement by Bennett [5], may also be described with POVM measurement as follows.

Let us consider two non-orthogonal states $|u\rangle$ and $|v\rangle$, and the angle θ between these two states, i.e., $\langle v|u\rangle = \cos\theta > 0$, see Figure 9.

The B92 protocol relies on the non orthogonality of the two states $|u\rangle$ and $|v\rangle$. Alice and Bob assign bit value `0` for $|u\rangle$, and bit value `1` for $|v\rangle$. Any operator may not discriminate these two states.

The B92 protocol is processed in a similar fashion as the BB84:

1. Alice chooses a bit `0` or `1` to be sent, prepares the corresponding state $|u\rangle$ or $|v\rangle$, and send it to Bob.

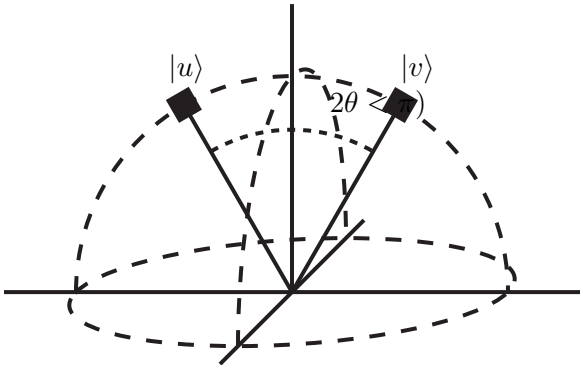


Figure 9: Two non orthogonal states used in the B92 protocol.

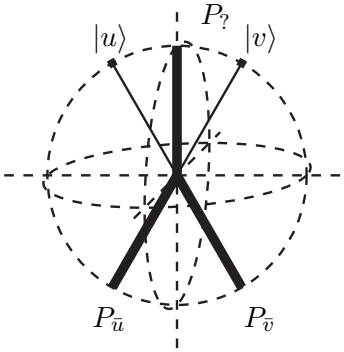


Figure 10: B92 POVM representation in the Bloch Sphere.

2. Bob applies the POVM described with the Equations (19-21).

3. Bob tells Alice on a public channel the states for which he has a positive outcome.

4. Alice and Bob keep only the corresponding bits.

It is also possible to build a table with states prepared by Alice and the measurement performed by Bob.

Table 2: All B92 states and measurements.

Bit to be sent	0			1		
Alice state	$\|u\rangle$			$\|v\rangle$		
POVM outcome	$P_{\bar{u}}$	$P_{\bar{v}}$	$P_?$	$P_{\bar{u}}$	$P_{\bar{v}}$	$P_?$
Detection Probability	0	$1-\cos\theta$	$\cos\theta$	$1-\cos\theta$	0	$\cos\theta$
Shared Bit Alice-Bob	No bit	0	No bit	1	No bit	No bit

The B92 protocol uses two vectors that may not be 100% separated, and BB84 uses two vector bases where vectors may be perfectly discriminated. It relies on a smaller number of states than the BB84, that makes it easier to build a prototype implementation. Moreover, there is no need of bases discussion, as Bob may determine directly what bit was sent when he has a positive outcome. The protocol is slower, however, as Bob may not obtain a useful result even when he chooses a measurement that could give him a positive outcome.

1.2.3 EPR, Squeezed States, and Continuous Variable Protocols

1.2.3.1 EPR states protocol

Ekert has described a cryptographic scheme in which Einstein-Podolsky-Rosen (EPR) pairs of particles [23]. are used to generate identical random numbers in remote places [24], while Bell's theorem certifies that the particles have not been measured in transit by an eavesdropper. Bennet described a related but simpler EPR scheme [8] and, without invoking Bell's theorem, proved its security against more general attacks, including substitution of a fake EPR source. This scheme is equivalent to the BB84 which uses single particles instead of EPR pairs.

1.2.3.2 Continuous Variable and Squeezed States Protocols

New quantum key distribution protocols types include light signals with much higher amplitude than single photon level energy. Homodyne detection is then used to measure the information of an electromagnetic mode quadratures. It is then possible to transmit a secret key with quasi-classical states [30, 31].

Schemes have been proposed using squeezed states [36, 28, 16]. In these schemes, the states are squeezed in one of two field quadrature components, and the value of the squeezed component is used to encode a character from an alphabet. The uncertainty relation between quadrature components prevents an eavesdropper from determining both with enough precision to determine the character being sent.

1.2.3.3 The 4+2: Combination of Advantages

The 4+2 protocol introduced by Huttner [40] presents advantages from both the two and four state protocols. By choosing non-orthogonal states, Alice and Bob take advantage of the two state protocol. That is, Eve may not differentiate in a deterministic way the two states of each basis.

The security of such a principle is based on two fundamental properties:

- The basis choice have to be completely hidden from the other party and from another Eavesdropper on the channel.
- When Alice and Bob use different bases, their bits are completely independent in a probabilistic manner.

The first property ensures that any eavesdropper that does not know the used basis will inevitably introduce errors in the transmission.

Though, this is necessary to verify conditions (5) and (13) as well as the condition:

$$\langle u_0|u_1\rangle = \langle v_0|v_1\rangle = \cos\theta > 0 \tag{25}$$

thus, $\theta < \pi/2$, and states from a same basis are in the same meridian plan in the Bloch sphere. An example of four states complying with these conditions is shown in Figure 11. The two measurements used in the 4+2 protocol are represented in Figure 12.

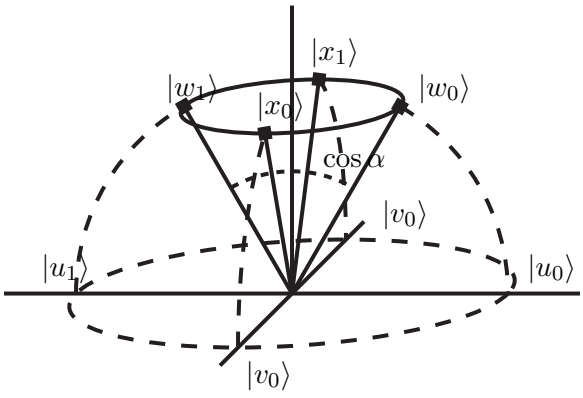
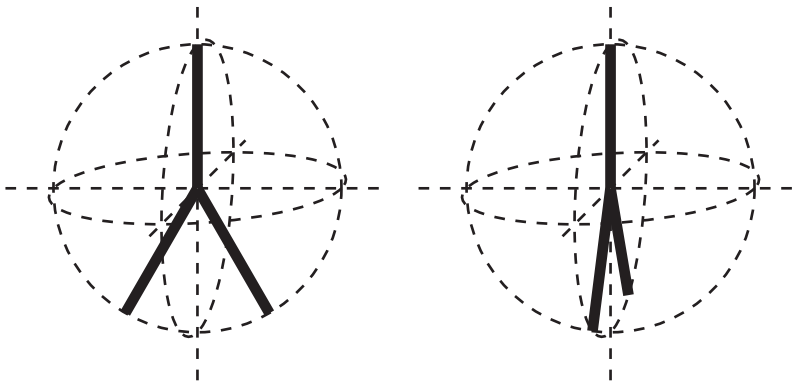


Figure 11: 4+2 Protocol states position in the Bloch Sphere.



(a) First POVM used to differentiate $|u_0\rangle$ and $|u_1\rangle$.

(b) Second POVM used to differentiate $|v_0\rangle$ and $|v_1\rangle$.

Figure 12: 4+2 Protocol POVM to distinguish same basis states.

1.2.3.4 SARG Protocol

One can also notice the existence of the SARG protocol [57, 1], developed by Acin, Scarani *et al.* This protocol differs from the original protocol by Bennett and Brassard (BB84) only in the classical sifting procedure. This protocol is provably better than the BB84 against the photon number splitting (PNS) attacks at zero error. Though, we will consider in this dissertation only hardware means to avoid the PNS attack.

1.3 Conclusion

Cryptography systems, developed over history, allow one to transmit secure data using encryption and decryption problem. Symmetric encryption schemes are fast and efficient and show a great security, as long as the encryption key is long enough and kept secret. If this key is as long as the message, the one time pad scheme may be applied for perfect security. Though, the secure key transmission problem between Alice and Bob remains.

In order to transmit securely the encryption key, public key algorithms make one part of the process publicly available, either encryption or decryption. Only people with the private key may proceed to the second part of the transmission, decryption or encryption respectively. These algorithms rely on mathematical conjectures, e.g., the difficulty to factorize the product of two large primes. Asymmetric algorithms are often slow. Moreover, a security threat remains as they are not 100% proven yet.

Quantum cryptography solves this problem and allows secure key transmission. Security of such a transmission is based on physical principles, not on mathematical conjectures. An additional security of such system is that transmissions may not be recorded and attacked *a posteriori*, because quantum transmission have the evanescent property that allows enhanced security.

Many quantum key distribution protocols exist, including the BB84 or the B92 protocol. We will study the theoretical security of such protocols, as well as the implementation of a prototype using a *strong reference* detection. A prototype will be implemented and tested in order to check its performance regarding data rate and security with respect to different attacks, and maximum reachable transmission distance between emitter and receiver.

CHAPTER II

INFORMATION, SECURITY, AND QUANTUM CRYPTOGRAPHY

Quantum key distribution solves a problem that classical cryptography cannot, i.e., secret growing between two remote parties, usually called Alice and Bob. The uncertainty principle of quantum physics is used to guarantee that no eavesdropper is tampering with the signal during the transmission. Quantum key distribution includes two main steps: the quantum preparation, transmission, and measurement of particles first and the classical *reconciliation* step second. This last step is a public discussion on a classical channel between Alice and Bob to extract a final key from the quantum discussion.

The non-cloning theorem [74] is the main tool used to prove security of a quantum key distribution system. It prevents any eavesdropper to listen to the quantum transmission without creating errors and remaining unnoticed. Imperfect devices may also introduce errors in the transmission, typically 10% of the bit string. To avoid any confusion with the error rate in classical communication, which is typically of the order of 10^{-9}, Beat Perny from Swisscom and Paul Townsend from British Telecom proposed to call the quantum transmission error rate, QBER, for quantum bit error rate [25].

To show secrecy for real transmission systems, we consider the worst case scenario: the observed QBER is assuming to be solely due to an eavesdropper. This spy is usually called Eve. She has access to perfect technology and complies to physical laws. Information may have leaked during the quantum transmission and error correction that Eve may have retain. A QKD protocol is then defined as being *secure* [52] if for any security parameter $\xi > 0$ and $\eta > 0$, Eve's mutual information with the final key, I_{Eve}, is less than ξ with a probability $1 - O(\eta)$. In other term, one can achieve the following criterion:

$$\text{Prob}\,(I_{\text{Eve}} > \xi) < \eta. \tag{26}$$

The purpose of this chapter is to show how QKD protocols, and more precisely QKD systems with laser sources may comply to the condition of Equation (26). The classical communication step between Alice and Bob to extract a final secure key is described in Section 2.1. Then, Section 2.2 studies attacks on the quantum communication step when Eve has access to perfect technology. Finally, the security of imperfect single photon sources is addressed in Section 2.3 and the use of a *strong reference* to prevent security threat is also discussed.

2.1 Classical Step and Secret Key

The quantum key distribution initial phase is the quantum transmission and basis disclosure to keep only correlated bits between Alice and Bob, see Section 1.2. Upon successful completion, they share a key of N bits, see Figure 13. With perfect systems, their keys are strictly identical. However, practical imperfections lead to errors between both keys. Alice and Bob proceed to a comparison to evaluate the QBER with a public authenticated channel. Then, they implement an error correction to produce two identical keys between them. In the most adverse case, Eve can replace the imperfect channel with a lossless error free channel and attacks the bits. As per the physics law, these observation introduce a disturbance and thus errors. These errors are completely due to Eve. Then, Alice and Bob apply privacy amplification to lower Eve's information to a level that can be arbitrarily small, see Figure 13.

This process may be stopped after QBER evaluation. If it is too high, Alice and Bob may decide to stop communication as the eavesdropper may retrieve enough information that prevents a secure communication.

Finally, quantum key distribution systems practical security depends on the desired security level, i.e., the acceptable assumptions that are made regarding today's technology. Quantum cryptography security may be used for security level up to *perfect secrecy*.

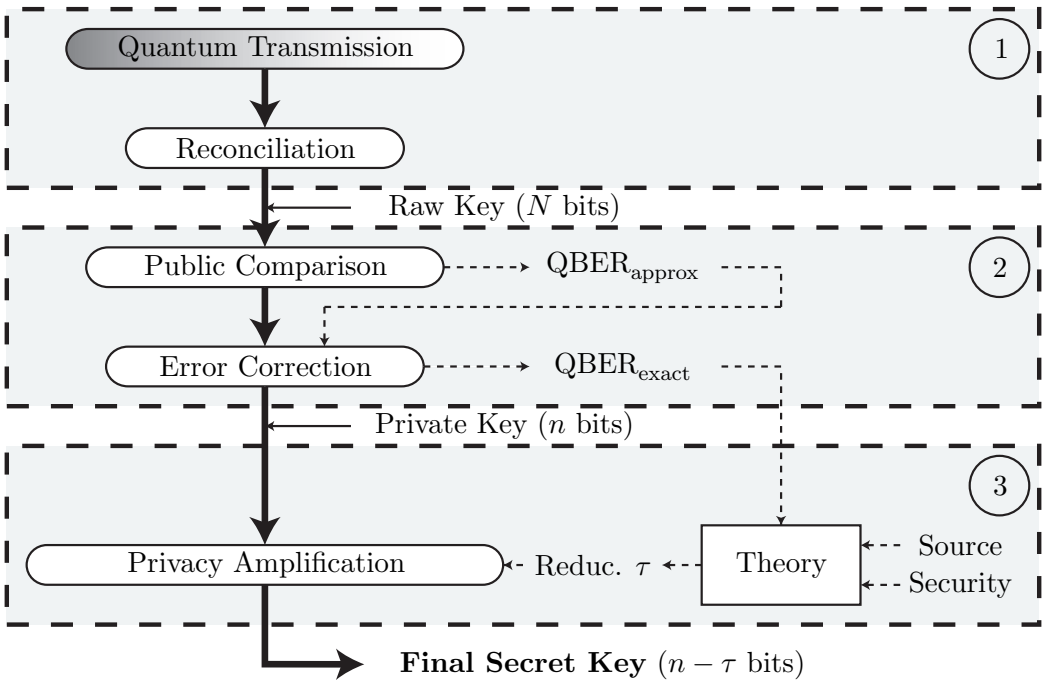


Figure 13: Quantum Key Distribution General Procedure Description. The three steps are 1) Quantum Communication and Reconciliation, 2) Comparison and Error Correction and 3) Privacy Amplification to have a final secret key.

2.1.1 Errors, Correction, and QBER

2.1.1.1 Public Comparison

The purpose of comparison is to give an error rate approximation between Alice's and Bob's bit strings. This step is performed with a public channel and breaks into three steps, see Figure 14:

- Random choice by Alice of key part to be compared KA_1.
- Public exchange of the key part KA_1 between Alice and Bob.
- Error rate computing by direct comparison using the public channel.

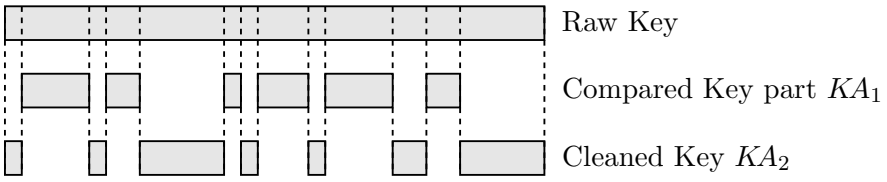


Figure 14: Different parts used in public key comparison.

The error rate of one part will be representative of the error rate of the other part with a very high probability. The error rate approximation quality depends on the amount of bit in KA_1. Suppose the key is broken into two random parts. Using [64], and assuming a key of length N, KA_1, KA_2, KB_1 and KB_2 the two key parts from Alice and Bob, and $d(K_1, K_2)$ the amount of errors between the two bit strings K_1 and K_2, it is then possible to show that for all δ and β such as $0 < \delta < (\delta + \beta) < 1$:

$$\text{Prob}\left\{\left(d(KA_1, KB_1) \leq \frac{\delta}{2}l\right) \cap \left(d(KA_2, KB_2) \geq \frac{\delta+\beta}{2}l\right)\right\} \leq e^{\frac{-\beta^2 N}{16(\delta+\beta/2)}}. \tag{27}$$

Then the remaining part quantum bit error rate is approximated by:

$$\text{QBER}_{\text{approx}} = N/d(K_1, K_2). \tag{28}$$

The amount of key to compare must be both low enough not to disclose too much of the key, and high enough to guarantee a good approximation of error rate and to adapt the error correction process.

To defeat an eavesdropper attack, the random choice of key KA_1 must be done *a posteriori* of quantum transmission. Otherwise, Eve could then observe the remaining key part (KA_2) without creating errors on the first part. The QBER estimation would be completely erroneous, preventing the process to be secure.

2.1.1.2 Error Correction

Error correction corrects errors on KA_2 and KB_2 keys to produce an identical key between Alice and Bob. They use a public channel to transmit information on the keys structures, called *syndromes*, than can locate and correct errors. The initial knowledge of the error rate is a crucial point for an efficient process.

We assume that each bit is transmitted independently with an error probability, QBER. The minimum amount of bits, r, that Alice and Bob need to exchange on the public channel to correct their errors is given by Shannon's coding theorem [72]. It satisfies:

$$r = n\left[-\text{QBER}\log_2(\text{QBER}) - (1-\text{QBER})\log_2(1-\text{QBER})\right]. \tag{29}$$

Shannon's proof does not give explicit error correction methods. Bennett and Salvail described an algorithm called **cascade** that approaches Shannon's limit. The protocol follows

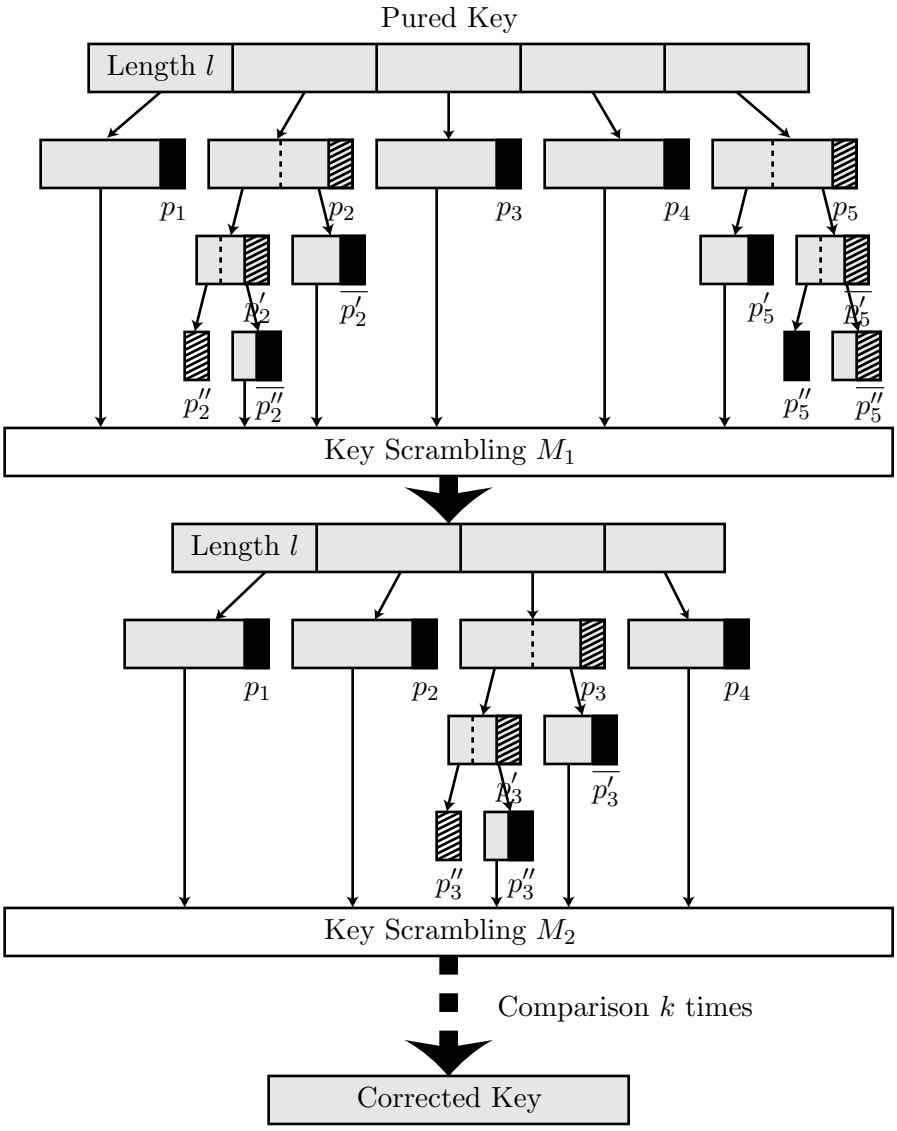


Figure 15: Parity Block Error Correction *Cascade* Protocol Principle. The key is split into l length blocks, and parities $p_1, p_2, p_3, ..., p_n$ are computed. A hatched block shows different parity between Alice and Bob. Blocks are kept without the parity bit, and scrambled with M_1. The process is renewed k times to give the final corrected key.

the steps, see Figure 15: Alice and Bob break their key into length l blocks, depending on the approximated QBER, $\text{QBER}_{\text{approx}}$. They compare the block parities $\{p_1, p_2, p_3, ..., p_n\}$ on the public channel. When parity does not match, the block includes an odd number of errors (p_2 error in the figure). Blocks with same parity are considered as good and stay unchanged. Blocks with different parity are split in two, and the parity of each part is then compared between Alice and Bob. The "good" half-block is kept, the other one is split into two, up to when the error is found. This communication reveals some information to Eve that is exactly 1 parity bit each time. The key is then scrambled with a matrix M_1 to find the errors that have not been detected at first pass. This process is repeated many times as a function of the error rate $\text{QBER}_{\text{approx}}$ and the number of corrected errors each time. The remaining error in the final key is exponentially small. The resulting key is then the same between Alice and Bob with a very high probability.

Contrary to original error correction described by Bennett *et al.* [6], this process does not discard any bit from the bit string. There exists more efficient protocols based on *syndromes* transmission between Alice and Bob [15].

Error correction gives the exact value of the initial error rate without revealing the key. While the errors that are assumed to be introduced by Eve, the information gathered by Eve is not eliminated. Alice and Bob can not use the key as is.

2.1.2 Privacy Amplification and Information

After the error correction, Alice and Bob have the same bit string, but that is not fully *secret*. They know the exact key initial error rate, $\text{QBER}_{\text{exact}}$. One can compute the amount of bits τ that the key must be reduced, so Eve's information drops below a threshold ξ [52].

This step is referred as privacy amplification. Alice chooses randomly a binary matrix M_τ of size $(n - \tau) \times n$ and transmits it to Bob on the public channel. The final key K_{final} is then:

$$K_{\text{final}} = M_\tau \cdot K_{\text{corrected}}. \tag{30}$$

The value τ may be evaluated based on the amount of information Eve has been able to retrieve. Consider that Alice's, Bob's and Eve's binary strings are random variables

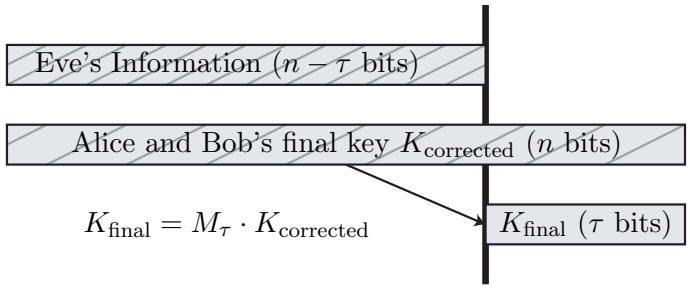


Figure 16: Privacy Amplification.

α, β and ε with joint probability density function $P(\alpha, \beta, \varepsilon)$. Alice and Bob have access to marginal density function $P(\alpha, \beta)$ from which they can deduct Eve's maximal information. Alice and Bob can then establish a secret key when [19]:

$$I(\alpha, \beta) \geq I(\alpha, \varepsilon) \text{ or } I(\alpha, \beta) \geq I(\beta, \varepsilon), \tag{31}$$

where $I(\alpha, \beta)$ is the Shannon mutual information between Alice and Bob, $I(\alpha, \beta) = H(\alpha) - H(\alpha/\beta)$ where H is Shannon entropy. In other words, it is possible to have a secret key when Alice/Bob share more information than Eve with either of them.

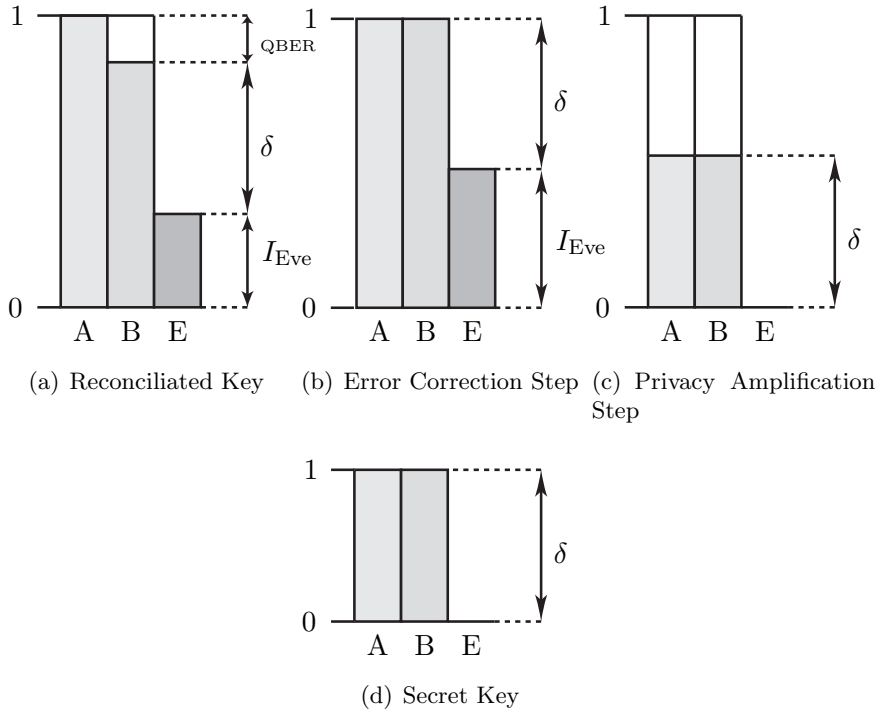


Figure 17: Intuitive representation Alice, Bob, and Eve's information.

It is possible to intuitively understand Equation (31) thanks to Figure 17. During error

correction step, Eve gains as much information as Bob does. Thus, the mutual information difference stays the same. After error correction, the Alice-Bob mutual information is equal to 1, see Figure 17(b). After privacy amplification, Eve's information is zero, see Figure 17(c). Finally, Bob reduces the key by discarding bits during the privacy amplification step. Alice and Bob share all secret information., see Figure 17(d).

2.2 Eavesdropping and Attacks on QKD.

It is now necessary to evaluate the maximum amount of information gathered by Eve for a given error amount observed on the channel. Attacks performed on the quantum channel may be split into different categories. When Eve performs an *incoherent* attack, she attacks each transmitted photon individually with a probe, i.e., a state prepared by Eve that will interact with the "attacked" state. She then stores it in a quantum memory to perform later further measurement, see Section 2.2.1. The second possible set of attacks are the *incoherent* attacks. Eve performs a unitary quantum operation on one of her probe and all the transmitted photons at the same time. Then Eve may gather a coherent information on the entire transmission, see Section 2.2.2.

2.2.1 Incoherent Attacks.

For incoherent attack, Eve attacks one transmitted photon after an other in a sequential manner, see Figure 18. One can study in a classical way this type of attack. Alice, Bob, and Eve have classical information modeled as random variables α, β and ε. Quantum physics laws decide on the joint probability density function $P(\alpha, \beta, \varepsilon)$.

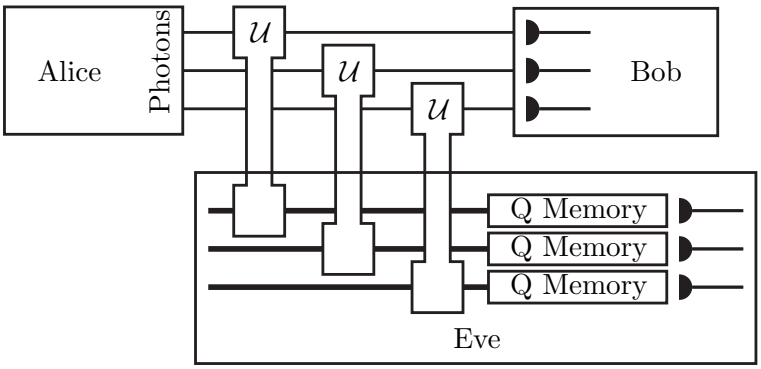


Figure 18: Incoherent Attack

2.2.1.1 Incoherent Attacks Maximum Efficiency

Eve generates a quantum state (probe) that will be use to interact with each photon on the quantum channel using a unitary transformation. The cloning machine attack is the best efficiency symmetric attack that Eve can perform. It gives maximum information to Eve, and for low QBER, the information gain grows linearly [25]:

$$I^{\max}(\alpha,\varepsilon) = \frac{2}{\ln 2}\mathrm{QBER} + O(\mathrm{QBER}^2) \approx 2.9 \cdot \mathrm{QBER}. \tag{32}$$

Bob's Shannon information is decreasing:

$$\begin{aligned} I(\alpha,\beta) &= H(\alpha) - H(\beta/\alpha) \\ &= 1 + \mathrm{QBER}\log_2(\mathrm{QBER}) + (1-\mathrm{QBER})\log_2(1-\mathrm{QBER}). \end{aligned} \tag{33}$$

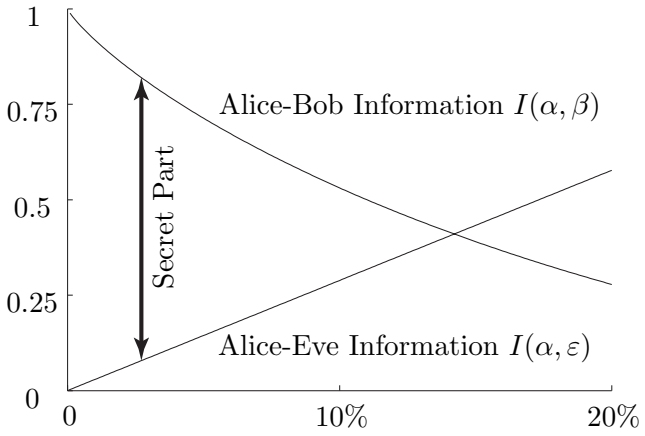


Figure 19: Eve-Bob information as a function of the QBER.

Curves from both Equations (32) and (33) are drawn in Figure 19. They cross QBER_0 where:

$$I(\alpha,\beta) = I^{\max}(\alpha,\varepsilon) \Longleftrightarrow \mathrm{QBER} = \mathrm{QBER}_0 = \frac{\sqrt{2}-1}{2\sqrt{2}} \approx 15\%. \tag{34}$$

The BB84 protocol is secure against any individual attack if and only if $\mathrm{QBER} < \mathrm{QBER}_0$. One can then proceed to classical privacy amplification to extract a secret key. Otherwise the transmission should be stop.

This threshold is derived for one-direction privacy amplification protocols. There exists some *advantage distillation* protocols using bidirectional communication, that have a maximum acceptable QBER of 30% [26].

2.2.1.2 Incoherent Attack Example: Intercept and Resend

For example of attack on the system, Eve measures the states sent by Alice on a random selected basis and sends prepared states to Bob that are exactly what she measured. This attack is called Intercept-and-Resend. Table 3 describes all possible cases corresponding to the selection of bases, bits, by Alice and Eve.

Table 3: Eve's Receive & Resend Attack. Eve is in the middle of the channel. ? shows a random measured result, - shows a discarded measured state. Half of the shared bits are random. The final error rate is 25%.

Bit to be send	0		1		0		1	
Base	U		U		V		V	
Alice	$\|u_0\rangle$		$\|u_1\rangle$		$\|v_0\rangle$		$\|v_1\rangle$	
Eve's Meas.	U	V	U	V	U	V	U	V
Outcome	0	?	1	?	?	0	?	1
Eve sends	$\|u_0\rangle$	?	$\|u_1\rangle$	?	?	$\|v_0\rangle$	?	$\|v_1\rangle$

Bob's Meas.	U	V	U	V	U	V	U	V	U	V	U	V	U	V	U	V
Shared bit	0	-	?	-	1	-	?	-	-	?	-	0	-	?	-	1

Half of Bob's string is shared by Alice. The second half though has been detected at random, half of it is then correct, half is false. In a perfect quantum channel, Eve does introduce 25% error on the final key. With this method, Eve gathers the maximum information on the transmission [39], but it creates a very high error rate above the acceptable 15% rate to extract a secret key between Alice and Bob.

2.2.1.3 Incoherent Attack Example: Breidbart Basis Measurement

The previous attack is also the most intuitive, as Eve performs the same measurements as Bob and sends back to Bob prepared states. Eve uses the correct basis only half of the time. She knows the exact bit when the correct basis is used.

For a more complex attack, she measures the bits in a intermediate basis shifted by θ compared to $|u\rangle$ and $|v\rangle$, see Figure 20. When angle shift is $\theta = \pi/8$, the basis is called Breidbart basis [6].

The mutual information between signals sent by Alice $X = \{0, 1\}$ and signal detected

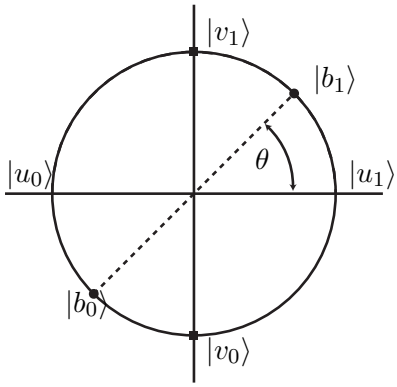


Figure 20: Measurement in the Breitbart basis.

by Eve $Y = \{|b_0\rangle, |b_1\rangle\}$ may be computed as follows:

$$I_{\text{Eve}}(X;Y) = H(Y) - H(Y/X). \tag{35}$$

As the repartition function of the bits sent by Alice is uniform, $p(X=0) = p(X=1) = \frac{1}{2}$, the entropy X is maximum:

$$H(X) = -\sum_{x \in X} p(x)\log_2(x) = -\left(\frac{1}{2}(-1) + \frac{1}{2}(-1)\right) = 1. \tag{36}$$

To evaluate the conditional entropy $H(Y/X)$, it is necessary to compute the detection probability of a sent symbol. For bit 0, Alice chooses randomly to send $|u_0\rangle$ or $|v_0\rangle$, then:

$$\begin{aligned} p_{|b_0\rangle/0} = p(|b_0\rangle/0) &= p(|u_0\rangle)p(|b_0\rangle/|u_0\rangle) + p(|v_0\rangle)p(|b_0\rangle/|v_0\rangle) \\ &= \frac{1}{2}cos^2(\theta) + \frac{1}{2}cos^2\left(\frac{\pi}{4} - \theta\right) \end{aligned} \tag{37}$$

We can evaluate $p_{|b_1\rangle/0}, p_{|b_0\rangle/1}, p_{|b_1\rangle/1}$:

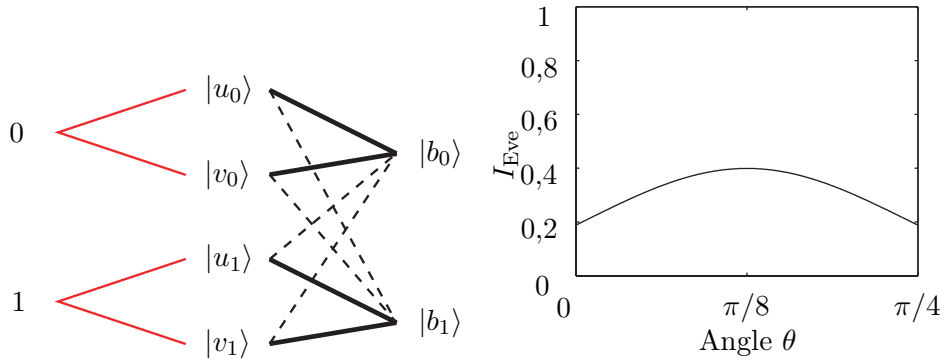
$$p_{|b_1\rangle/0} = \frac{1}{2}sin^2(\theta) + \frac{1}{2}sin^2\left(\frac{\pi}{4} - \theta\right), \tag{38}$$

$$p_{|b_0\rangle/1} = \frac{1}{2}cos^2(\theta) + \frac{1}{2}cos^2\left(\frac{\pi}{4} - \theta\right), \tag{39}$$

$$p_{|b_1\rangle/1} = \frac{1}{2}sin^2(\theta) + \frac{1}{2}sin^2\left(\frac{\pi}{4} - \theta\right). \tag{40}$$

The conditional entropy $H(Y/X)$ may be expressed as:

$$\begin{aligned} H(Y/X) &= -\sum_{x \in X} p(x) \sum_{y \in Y} p(y/x)\log_2(p(y/x)) \\ &= -p(0)\left[p_{|b_0\rangle/0}\log_2(p_{|b_0\rangle/0}) + p_{|b_1\rangle/0}\log_2(p_{|b_1\rangle/0})\right] \\ &\quad - p(1)\left[p_{|b_0\rangle/1}\log_2(p_{|b_0\rangle/1}) + p_{|b_1\rangle/1}\log_2(p_{|b_1\rangle/1})\right] \end{aligned} \tag{41}$$



(a) Eve's Binary channel (b) Mutual Information

Figure 21: Eve's binary channel and mutual information.

The mutual information I_{Eve} is sketched in Figure 21(b).

The maximum information gain is for $\theta = \pi/8$, which corresponds to the Breidbart basis. Mutual information is then $I_{\text{Eve}} \approx 0.399123$. For the Intercept and Resend attack, Eve detects every other time the correct bit value so her average information gain is 0.5 bit. The Intercept and Resend Attack is more efficient then the Breidbart basis one.

For the Breidbart basis attack, Eve is able find the correct bit value with a 85% probability vs. 75% for the intercept and resend attack. This comes from the intercept and resend attack that gives a deterministic value of the transmitted bit. For the Breidbart base attack, we are always 85% sure that we have the correct bit value, that is thus a probabilistic measure of the transmitted bit.

2.2.2 Coherent, Joint, and Collective Attacks.

Coherent attacks, also called *joint* attacks, are the most general where the photons can be measured at the same time and the measurements are processed at one, see Figure 22. A more restrictive set is called *collective* attacks, uses a probe for each sent photon, and then all probes are processed at the same time with a quantum computer, see Figure 23.

2.2.2.1 Coherent or Joint Attacks

For coherent attacks, Eve uses a single high dimensional probe on all the photons at the same time. She keeps it in a quantum memory until after the public discussion, see Figure 22. She then performs a measurement to gather maximum information. The most general

measurement class is the POVM measurement class [53].

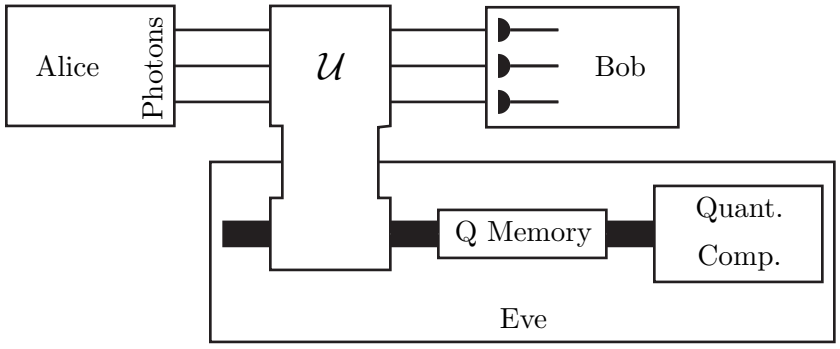


Figure 22: Coherent Attack. Eve uses a high dimension probe that interacts with all photons sent by Alice. She keeps it in a quantum memory until all bases are revealed.

When Alice sends n qubits, Eve gathers the information $I(\alpha;\varepsilon)$ and Bob gains the information $I(\alpha;\beta)$. We can write:

$$I(\alpha;\varepsilon) + I(\alpha;\beta) \leq 1. \tag{42}$$

This may be intuitively understood because Eve and Bob may not receive together more information than Alice sent [25]. With Equation (31), the condition to extract a secret key is $I(\alpha;\beta) \geq 1/2$, i.e., with using the Alice-Bob information as a function of the QBER:

$$\mathrm{QBER}\log_2(\mathrm{QBER}) + (1-\mathrm{QBER})\log_2(1-\mathrm{QBER}) \leq \frac{1}{2}. \tag{43}$$

which implies: QBER $\leq$11% [47, 62].

The 11% threshold is compatible with the 15% given for incoherent attacks, see Section 2.2.1. The 15% threshold is necessary because there exists an explicit strategy that reaches this limit. Though, if one suppose that Eve does not have the possibility to build a probe that she may entangle no more than n_0 photons, $n_0 < n$, then there is a very negligible probability that errors may come from Eve tapping in the channel. Thus, the 15% threshold is still valid [17, 4].

2.2.2.2 Collective Attacks

Collective attacks ar close to incoherent attacks because one probe per sent photon is used. Eve may then use a POVM on all probes at the same time, considered then as a single large quantum system, see Figure 23.

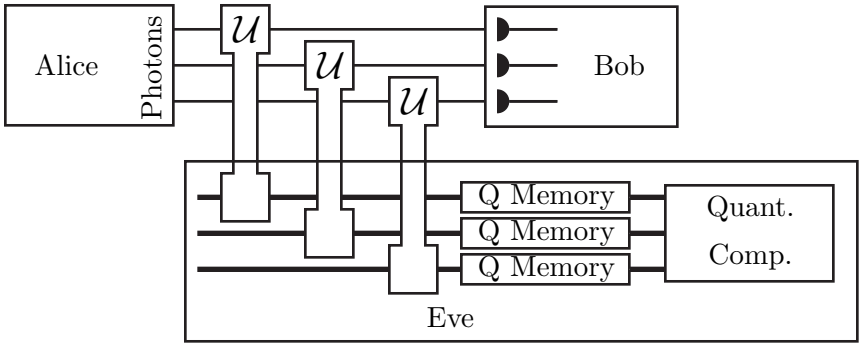


Figure 23: Collective Attack. Eve uses a high dimension quantum computer to process all probes at the same time.

Only protocols using linear error correcting codes are considered in security proofs [9].

2.2.3 Practical and Theoretical Security

The security of a whole system must be studied under different aspects. Let consider first the theoretical security. Quantum cryptography comes in where classical cryptography fails, that is secret growing between remote parties. It is then possible to prove quantum cryptography absolute security, even in the presence of noise and technological imperfections. This security comes with a price. However, it is also not realistic to consider that a spy has perfect technology to tap in the channel. We will also consider the financial cost as a function of the desired security level.

2.2.3.1 Authentication

The quantum key distribution process is very sensitive to the man in the middle attack. Eve places herself in the middle of the transmission link. She cuts the channel, then she acts as Bob toward Alice and as Alice toward Bob, see Figure 24. Eve is now as a transparent relay and knows all information going between Alice and Bob. It is then necessary that Alice and Bob use authentication, i.e., they must be able to guarantee that the messages have not been modified through the channel, by Eve for example. This step assures to be immune versus the man in the middle attack.

Alice and Bob need only to authenticate the final key to guarantee that the whole process has not been compromised. This step may be performed on the classical channel.

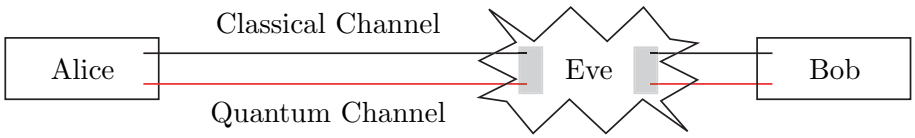


Figure 24: Man in the middle Attack. Eve places herself in the middle of the link and spoofs both Alice and Bob.

Many classical cryptography techniques perform authentication when Alice and Bob share some initial secret K_{auth} to *sign* the classical transmission.

The initial secret key K_{auth} is exponentially smaller than the new key K_{secr} generated with the QKD system, but long enough to enable authentication. Alice and Bob may use an algorithm described in [71] with their initial secret key to generate a signature T, that enables to check the authenticity of the message. Alice and Bob may keep part of the new key to perform the authentication of the next QKD session. If Eve does not have knowledge of the initial shared secret between Alice and Bob, she cannot interfere on the authentication signature T. She would be detected by Alice and Bob.

It may look like a paradox that one need an initial secret to establish another secret. Though, the necessary amount of secret for authentication is much less than the final generated secret. As a result, quantum key distribution is much more about secret growing than strictly key exchange.

2.2.3.2 Trojan Horse Attack

Up to now, Eve is trying to gain information by observing and working on the transmitted qubits on the quantum channel. She may operate in a completely different way by using the quantum channel itself to break into Alice and Bob's apparatus. For example, she sends an optical signal directly toward Alice or Bob to observe the inducted reflections. This strategy is called *Trojan horse attack*. The reflected signal analysis may then give information on the system current state, modulators state, polarizer state, or anything that encodes the information.

It is possible to argue that filters and circulators may avoid reflections, and thus, drastically reduce the amount of information gathered by Eve. This is possible because Alice

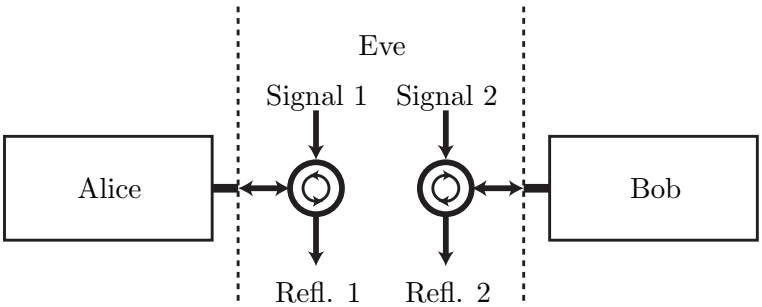


Figure 25: Trojan Horse Attack.

and Bob are using only a one way quantum communication, so Alice may block incoming signals, and Bob blocks outgoing signals.

Once one assumes that Eve has no limitation other than theoretical ones, while Alice and Bob may be faced with technical limitations, Eve may be able to gain access to some information. Such paradigm brings quantum cryptography into the discussion regarding scientific assessment of secrecy *vs.* technically achievable secrecy

2.2.3.3 Theoretical Security and Practical Cost

Quantum physics principle may be challenged by a new theory. Though, it is reasonable to consider that today's description will still stand for a photon transmitted over an optical fiber. This is the same for the Newtonian physics that describes planets trajectories or apple falls. After all, transmission security may not rely only on theoretical quantum physics properties. Today's implementation has it own limitations.

Despite the elegance and generality of security proofs, the idealness of quantum cryptography system whose security relies entirely on quantum principles is unrealistic. Abstract concepts implementation will be always jeopardized. This may still be the weak point of all systems. Moreover, one should always keep in mind that infinite secrecy requires infinite cost and has an almost zero interest.

There are two important advantages for quantum cryptography. First of all, it is much easier to broadcast technological than mathematical progress. The threat that quantum cryptography may be broken overnight is negligible, but this is not the case for public key

cryptosystems. Then, quantum cryptography security depends on the adversary technological level *at the time of the key exchange*. Though, for classical systems, the message may be recorded and broken using future advances in cryptanalysis. This last point is very useful for secrets that need to last for years.

A significant advantage for quantum cryptography is its sensitivity to *today*'s technology. It is impossible for an eavesdropper to perform an attack after the transmission *a contrario* classical transmission, where it is easy to read and record the encrypted information to decipher it later.

A possible answer to today's very high security need is to use quantum key distribution with classical symmetric algorithms such as AES at the same time, for which a frequent encryption key enables a quasi-perfect security level, see Figure 26.

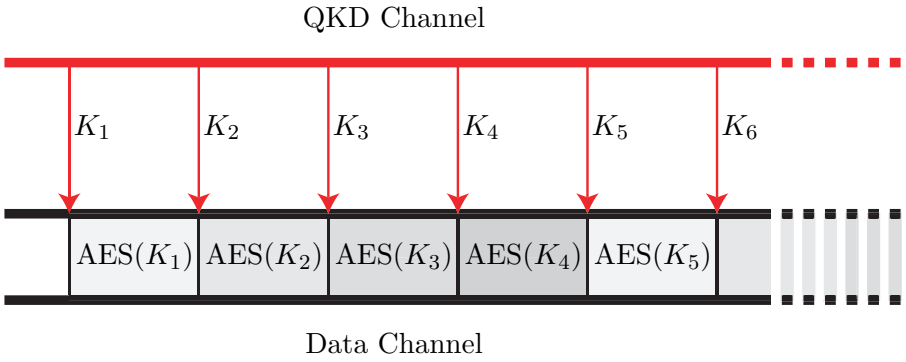


Figure 26: Encryption key use.

2.3 Imperfect photon sources and PNS Attack

Quantum key distribution protocols based on BB84 need a perfect single photon source to have unconditional security. Ideal single photon source are today not available, one must then study the security of imperfect sources. Eve may perform an attack by gathering a photon when the pulse does contain more than one photon. This attack is called the photon number splitting attack (PNS attack), Eve gains information without disturbing the signal. This attack will be specifically studied with a fainted laser that outputs a significant amount of multiphoton pulses, see Section 2.3.1.

A solution proposed by Huttner is to use a *strong reference* in the system [40]. The

amount of information gathered by Eve is a function of the initial average power, one can then compute the maximum possible amount of secret information to be extracted, see Section 2.3.2.

2.3.1 Single Photon Source and PNS Attack

We will study how multiple photons in a single pulse, combined with a lossy channel and an imperfect detector may impact security. However, Eve is only limited by physics and has access to perfect technology, perfect translucent fiber or perfect single photon source for example. Quantum non-destructive (QND) measurement photon number measurement complies to physics laws and gives the possibility for Eve to count the number of photons in a pulse without disturbing them. She may then use this measurement to attack pulses containing more than one photon.

2.3.1.1 Fainted Lasers and Multiphoton Pulses

Today's QKD prototypes use fainted lasers. They produce a coherent state $|\Psi\rangle$, a pure k-photons states mix. By using a pulsed laser with initial average energy μ, the probability to have exactly k photons $p_\mu(k)$ in a pulse is:

$$p_\mu(k) = \frac{\mu^k e^{-\mu}}{k!}. \tag{44}$$

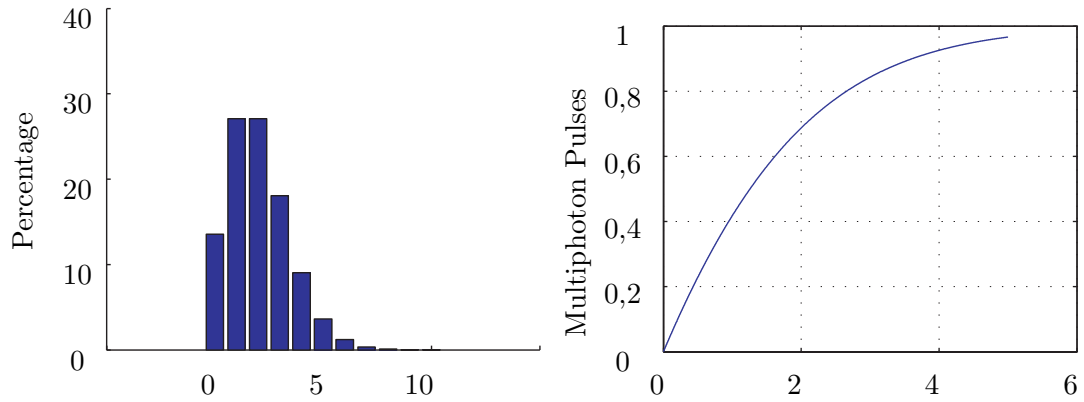
For μ=2, the ratio of pulses with k photons is then $p_0 = 0.135, p_1 = 0.271, p_2 = 0.271, ...$, see Figure 27(a).

The state of ω_0 frequency and Φ phase laser pulse may be described as the superposition of multiphoton states with probability $p_\mu(k)$ for each state with k photon:

$$|\Psi\rangle = \sum_{k=0}^{\infty} \sqrt{p_\mu(k)} e^{j(\omega_0 t + \Phi)} |k\rangle \tag{45}$$

where $|k\rangle$ is a ground state with k photons. The ratio of multiphoton pulses $p_\mu(k \geq 2)$ over pulses having at least one photon $p_\mu(k \geq 1)$, see Figure 27(b), is then:

$$\frac{p_\mu(k \geq 2)}{p_\mu(k \geq 1)} = \frac{\sum_{k=2}^{\infty} p_\mu(k)}{\sum_{k=1}^{\infty} p_\mu(k)} = \frac{1 - p_\mu(k=0) - p_\mu(k=1)}{1 - p_\mu(k=0)} = \frac{1 - e^{-\mu} - \mu e^{-\mu}}{1 - e^{-\mu}} \approx \frac{\mu}{2}. \tag{46}$$



(a) Amount of k photon pulses for $\mu = 2$.

(b) Multiphoton pulses percentage as a function of initial average number of photon per pulse μ.

Figure 27: Multiphoton Pulses.

A laser source is far from being a perfect single photon source. When a low energy level is chosen, there are few multiphoton pulses, but the number of single photon pulses is also very low. It is then a very low efficiency source. If we use a more important energy level, most of the pulses include more one photon, but many pulses include also more than one photon. Thus, this is not a perfect single photon source.

Pulses that contain more than one photon contain several photons bearing the same encoded information. Many copies of the same photon are then directly accessible to Eve. The PNS attack in an efficient attack that uses these characteristics.

2.3.1.2 The PNS Attack

Eve performs a non destructive measurement to determine the number of photons in each pulse and remains unnoticed. Eve thus knows the number of photons in the pulse without disturbing it. When the pulse contains more than one photon, she steals one. She keeps it in a quantum memory; this photon is in the same quantum state as the others in the pulse. Eve forwards the remaining photons to Bob thanks to a perfect translucent lossless fiber, see Figure 28.

After Alice and Bob publicly reveal their prepared and measured bases, Eve may perform her measurement in the correct basis. She gains a deterministic value of the encoded bit. When the pulse contains only one single photon, either she blocks it, or she forwards it

to Bob. Such choice is made as a function of the amount of pulse that Bob is awaiting. For a fiber distance d, the amount of pulse at Bob's input equals the number of pulses at Alice's output attenuated by the fiber, with losses $10^{-\frac{\alpha d}{10}}$, with $\alpha = 0,25\text{dB/km}$ for standard monomode fiber. Beyond the critical distance d_0, Eve forwards to Bob only the multiphoton pulses from which she kept one photon.

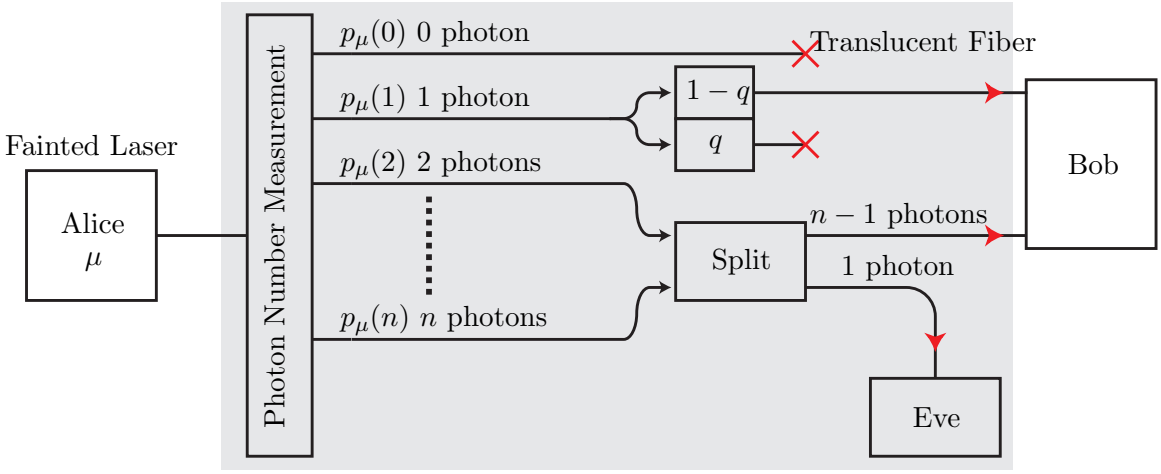


Figure 28: PNS Attack Principle

Though, if Alice and Bob decide to run a transmission for a distance shorter than d_0, Eve must make sure that Bob receives the same amount of pulses attenuated by the fiber, $\left(1 - e^{-\mu \cdot 10^{-\frac{\alpha d}{10}}}\right)$, to not be detected. Eve blocks only a part q of the pulses containing a single photon, to adjust the number of pulses received by Bob. This quantity q depends on the distance d between Alice and Bob and must satisfy:

$$p_\mu(k \geq 2) + (1-q) \times p_\mu(k=1) = p_{\mu'}(k \geq 1), \tag{47}$$

With $\mu' = \mu \cdot 10^{-\frac{\alpha d}{10}}$. Then, the amount of blocked pulses q is expressed as a function of distance d and initial energy μ:

$$q(d,\mu) = 1 - \frac{p_{\mu'}(k \geq 1) - p_\mu(k \geq 2)}{p_\mu(k=1)}. \tag{48}$$

The amount of information the Eve knows, see Figure 29, I_{Eve} is a function of q, thus a function of distance d and initial average energy μ:

$$I_{\text{Eve}}(d,\mu) = \frac{p_\mu(k \geq 2)}{p_{\mu'}(k \geq 1)} = \frac{1 - e^{-\mu} - \mu e^{-\mu}}{1 - e^{-\mu \cdot e^{-\frac{d\alpha}{10}}}}. \tag{49}$$

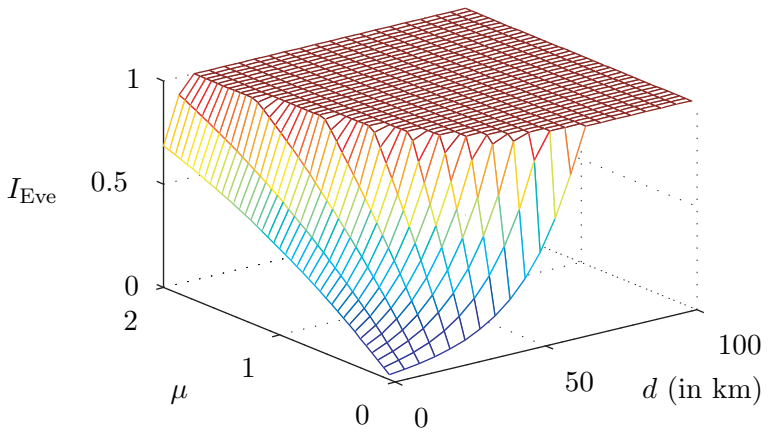


Figure 29: Eve's information I_{Eve} as a function of distance d between Alice and Bob. $\alpha = 0.25$dB/km.

Eve's information is a function of both variables d and μ. Eve's information must be lower than 1, to enable Alice and Bob to extract a secret from the shared information they have. On Figure 29, the operating points are located in the valley. The plateau corresponds to high energy μ and high distances d, where Eve has all the information that Bob has. The acceptable area is located for low μ and small distances. To authorize secret extraction over long distances d, it is necessary to use an exponentially small energy μ.

The space (μ, d) is split into two regions, where it is possible to extract a secret or not, from the top line that corresponds to critical distance d_0, that is distance over which Eve knows all the information, i.e., $q = 1$, as a function of initial average energy μ, see Figure 30. Distance d_0 may be expressed as a function of μ:

$$d_0(\mu) = -\frac{10}{\alpha} \ln[\ln(1-\mu)]. \tag{50}$$

For standard monomode fiber with average energy 0.1 photon per pulse, critical distance is 52km [1], which is very low compare to standard telecom distances. For over 40km transmission, and not to compromise security, Eve has half the Alice-Bob information; they must extract secret information from the key. Moreover, the 0.1 photon per pulse energy level limits the final bit rate.

The use of fainted laser, or more generally an imperfect single photon source, opens a security gap. Using the PNS attack, Eve may know an important part of the information. Though, the PNS attack requires a perfect translucent fiber. Such device is not available

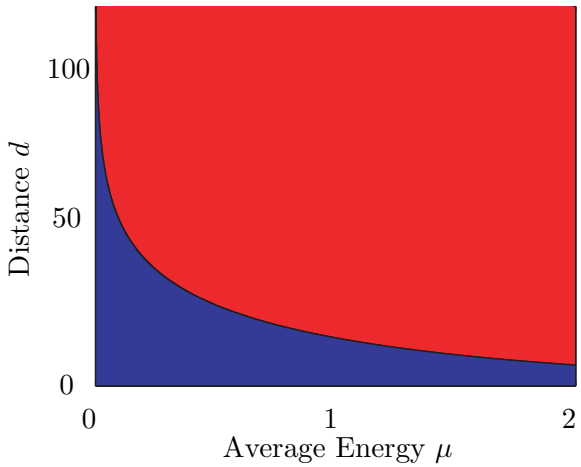


Figure 30: Possible secret communication area with a fainted laser source. Secret extraction is possible in the blue area. The red zone corresponds the values where Eve knows all the information (when $\alpha = 0.25$dB/km).

with today's technology[1]. Moreover, Raleigh and Raman diffusions impose a limit to performance of glass fibers. Eve must find a new technology that authorizes such translucent fiber to perform the PNS attack.

2.3.2 Reference and Reference Protocol

Multiphoton pulse combined with lossy fibers limit security. Eve may even retrieve all Alice-Bob information when they are separated from a distance larger than d_0. The PNS attack relies on the fact that Bob may not determine the origin of the signal "loss". A pulse containing no photon may have multiple origins: a pulse that indeed did not contain any photon at Alice's output, or a pulse that contained one or more photons, but has been stopped by the fiber attenuation. This uncertainty benefits Eve that can simply block the pulses, without being detected by Bob, thus, without being caught.

A proposal to avoid such security breach is to prevent Eve to be undetected when she blocks a pulse. Huttner proposed to include in the signal a reference that will be always detected [40]. It forces Bob to detect the reference at the same time as the pulse, guaranteeing that the pulse has been sent from Alice to Bob, even if Bob may not detect some information signal. A last argument given Lütkenhaus [46] is the robustness of such an

[1] Well, Q may have one in his tool kit

implementation because the absence of reference would indicate that Eve is in the system. The implementation of a strong reference in the system guarantees that the communication is secure against the PNS attack for any distance.

A *strong reference* must fulfill two conditions:

1. The reference must always be detected in the signal.

2. The reference must be intertwined with the signal. It should not be possible to have a reference signal without information signal.

2.3.2.1 Eve's Information with a Reference and Optimum Energy

When Eve performs a PNS attack, she gathers information extracted from multiphoton pulses without disturbing the signal. Those are the only one pulses from which she can gain information without disturbing the signal. When Bob is at a distance d from Alice, he receives only $(1 - e^{-\mu'})$ pulses, where $\mu' = \mu \cdot 10^{-\frac{\alpha d}{10}}$.

As all pulses are attenuated in the same way, the proportion of detected pulses that contain k photons is the same as initial proportion at distance $d = 0$. Multiphoton pulses known by Eve represent the same ratio as initial $p_\mu(k \geq 2)$, at any distance d from Alice to Bob. The proportion of bits known by Eve is a function of μ

$$I_{\text{Eve}}^{\text{ref}}(\mu) = \frac{p_\mu(k \geq 2)}{p_\mu(k \geq 1)} = \frac{1 - e^{-\mu} - \mu e^{-\mu}}{1 - e^{-\mu}} \tag{51}$$

Eve's information as a function of the initial average energy μ may be sketch in Figure 31.

Eve's information is a function of only one variable μ. It depends only on distance d. To be able to extract secret information from the transmission, it is still necessary to be in an area where Eve's information is lower than 1. This is always the case now the amount of information that Eve may know is always known and lower to Bob's information. Then, any μ is suitable for secret transmission. For high initial average energy, $\mu \geq 2$, Eve's information is high, and privacy amplification must be performed to reduce Eve's information.

Privacy amplification to reduce the information known by the PNS attack forces to reduce from an initial length n_0 to a new length $n = n_0 - \tau_0$:

$$n = n_0 - \tau_0 = n_0 \left(1 - I_{\text{Eve}}^{\text{ref}}\right) = \frac{n_0 \mu e^{-\mu}}{1 - e^{-\mu}}. \tag{52}$$

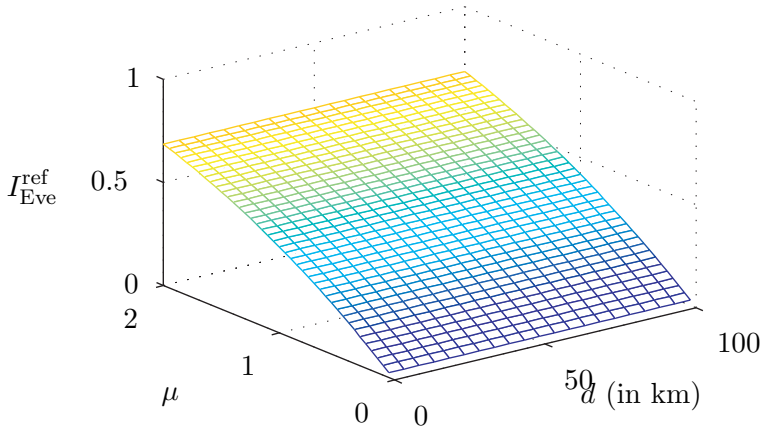


Figure 31: Eve's Information $I_{\text{Eve}}^{\text{ref}}$ with a strong reference is only a function of the Alice-Bob distance d, with $\alpha = 0.25\text{dB/km}$

Initial key length n_0 is proportional to the number of pulses received by Bob that contain at least one photon:

$$n_0 = N_0 \cdot p_\mu(k \geq 1) 10^{-\frac{\alpha d}{10}} = N_0(1 - e^{-\mu}) 10^{-\frac{\alpha d}{10}}, \tag{53}$$

where N_0 is the initial pulse frequency of pulses generated by Alice.

Thanks to Equations (52) and (53), the final key length n is proportional to $\mu e^{-\mu}$ that is exactly the probability $p_\mu(1)$ to have exactly one photon in a pulse.

The information gathered by Eve may not be amplified because Bob detects the reference for all pulses. For long distances, the reference may also be attenuated, that may the benefit Eve, who may then lower also the reference signal that she sends back to Bob, and thus, attenuate the generated error.

2.3.2.2 Maximum Bit Rate with a Laser Source

To have a maximum length final key, one must optimize the initial average energy value μ. The probability $p_\mu(1) = \mu e^{-\mu}$ shows a maximum for $\mu = 1$, see Figure 32.

The presence of a *strong reference* makes the system resistant to the PNS attack. Secret information that Bob may gather comes from single photon pulses sent by Alice, that is why optimum average initial energy μ to be used is $\mu = 1$.

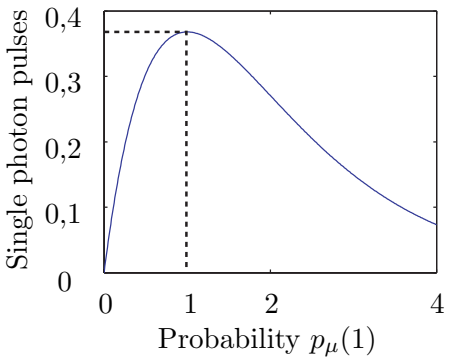


Figure 32: Probability to have exactly one photon in a pulse. One can observe a maximum for $\mu = 1$.

2.3.2.3 PNS Attack and Error Rate

When Eve performs the PNS attack, she does not create any error. In presence of errors in the practical system, we must assume that all these errors come from Eve tapping in the signal to gain information on the transmission. Her best strategy is to perform a PNS attack first on the multiphoton pulses, and then to perform an optimum incoherent attack or a coherent attack is she has access to the required technology. Thus, she will create errors, but only on part of the photons observed by Bob. The final observed error rate must be considered as coming only from the $p_\mu(1)$ part of the key.

For example, if Alice uses initial average energy $\mu = 1$, then, $p_1(1) = 0.368$ and $p_1(k \geq 2) = 0.264$ and $I_{\text{Eve}} = 0.418$, thus lower as the overall error generated by Eve. Privacy amplification described in Section 2.1.2 must be performed with a 6% QBER to compute an adequate τ reduction coefficient.

2.4 Conclusion

Quantum key distribution uses first a quantum channel. Alice prepares quantum particles and sends them to Bob to the other end of the quantum channel. Quantum physics measurements of uncertainty must be precise with a classical communication on the authenticated channel. Alice and Bob proceed then to the following steps, reconciliation, comparison, error correction, and privacy amplification to finally extract a secret key.

Quantum communication security, in case of no errors, is straight forward. Though,

errors may due to technological imperfection in used physical systems. To reach a perfect secrecy level, we consider that all errors are due to an eavesdropper tapping in the signal and invariably creating errors.

Eve may perform two different types of attack on the system. Incoherent attacks where particles are attack one after the other and coherent attack where all the particles are attacked as a whole quantum system. The maximum acceptable error rate is then 15% and 11% respectively for each attack type, from which Eve does know all information on the channel.

Shannon's information theory proves that with one time pad algorithm [68], the communication is perfectly secure. On a practical point of view, very high security level may be reach by using a quantum channel to generate continuously encryption keys that is then renewed as a seed for a more complex cryptographic application. It becomes very difficult to break the system because the key is used for a very short period of time.

Quantum cryptographic systems security may be perfect even when using non perfect single photon sources. Eve can then perform a PNS attack to gather information from the multiphoton pulses. This attack may be blocked with a *strong reference* detection in the system. It is possible to use a fainted laser and still perform a secret communication, with an optimum average energy per pulse to be one photon per pulse.

CHAPTER III

CRYPTOGRAPHY AND FREQUENCY CODING: THE SSB SYSTEM

The very seducing idea of using quantum cryptography for transmission in a full security manner was born thanks to Wiesner in the early 80's. In 1984, Bennett and Brassard proposed a protocol [7] for quantum key distribution. This concept stayed then very marginal. The scientific community did not give much heed to this theory. In 1992 with the first prototype developed by Bennett *et al.* [6], quantum cryptography started to draw significant attention.

The first experimentation used photon polarization to encode information in free space. More experiments have been performed on optical fibers, where bits are encoded with photon phase. Longer and longer distances are reached and are now over 100km [27]. This section presents different coding methods, and introduces the SSB system developed by Merolla *et al.* at the GTL-CNRS Telecom Laboratory, which serves as a starting point for work of this thesis.

Quantum key distribution protocol implementation requires, for maximum efficiency, a single photon source and perfect quantum detectors. Current technology limits such devices. Thus, practical approximation is a fainted pulsed laser source, which is very easy to implement, but has the inconvenience to generate multiphoton pulses as seen in Section 2.3. A reference protocol may be used to guarantee confidentiality even with multiphoton pulses. We will show in this chapter the implementation of such a reference.

3.1 Quantum Cryptography Experiments

Quantum cryptography protocols use a specific quantum state variable to encode information. Different variables of photon state $|\Psi\rangle$ may be used, considering the transmission medium and external physical constraints. Two variables are used in quantum cryptography

to encode information: polarization and phase.

This section describes, first, systems using polarization, mainly for free space transmission, then systems developed on optical fibers use phase.

3.1.1 Polarization and Information Encoding

Polarization to encode information may be used to implement the BB84 protocol [7]. Let consider four polarization states, horizontal →, vertical ↑, diagonal right ↗, and diagonal left ↖. These polarization states may be represented on the Poincaré sphere [52], see Figure 33.

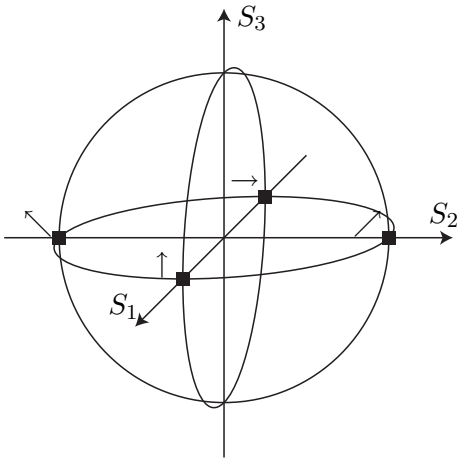


Figure 33: Polarization States on the Poincaré Sphere.

With a polarization crystal, it is possible to distinguish two polarizations that are opposed on the Poincaré sphere, for example → from ↑, or ↗ from ↖. These states are grouped into two bases horizontal-vertical (+) and diagonal (×). In these bases, photon polarization may be exactly determined. When the cube is aligned with basis +, it is possible to separate exactly polarizations ↑ and → on the two cube outputs. In the same way, it is possible to separate exactly polarizations ↗ and ↖ in basis ×. When a photon is not polarized in the corresponding basis, it is impossible to determine its initial polarization with a cube aligned with the other basis. The outcome of the cube is then randomly either of the two polarizations.

For the BB84 protocol, we consider that polarization → and ↑ are states $|u_0\rangle$ and $|u_1\rangle$ from basis U, and ↗ and ↖ are states from basis V. We then have the polarization

equivalence table for BB84 states, see Table 4.

Table 4: Polarization Equivalence Table.

Basis	U: +	V: ×
States	$\|u_0\rangle$: ↑	$\|u_0\rangle$: ↗
	$\|u_1\rangle$: →	$\|u_1\rangle$: ↖

The following quantum cryptography system uses polarization following this encoding table.

3.1.2 Polarization Encoding Experiments

3.1.2.1 In Free Space: From 32cm to 23km

In 1992, with the first experimental quantum key distribution, Bennett and Brassard communicated over 32cm of free space with polarization information [6], see Figure 34.

Figure 34: First Quantum Key Distribution Prototype over 32cm of Free Space.

Polarization is widely used for free space transmission, because air enables low dispersion and non-birefringence. This is also a simple and reliable method in terms of stability. It is then possible to use a 800nm wavelength, where losses are low, and for which detectors have a 50% efficiency. Alice uses a fainted laser to generate photons. Polarization encoding is performed with Pockels cells to force polarizations $\uparrow, \rightarrow, \nearrow, \nwarrow$ that correspond to the four BB84 states. The measurement uses a polarization cube and two photon detectors.

Buttler implemented a 1km transmission at Los Alamos laboratory [14, 13]. Then, a 10km distance in daylight was reached in 2002 [38]. John Rarity and Tapster performed a free space transmission on a 23.4km link in 2002 [55, 45].

Free space transmission systems have the advantage to be quickly and easily deployed. It is also possible to transmit information to satellites in low orbits and in a secure fashion. Ground transmissions are sensitive to air turbulence that leads to optical beam instability, thus increasing the transmission error rate [3].

3.1.2.2 Development of Optical Fiber Transmissions

Experiments have then been performed on optical fibers. The Geneva *Groupe de Physique Appliquée* (GAP) built a transmission system over 1km [11]. This apparatus was an upgrade of a previous prototype [50]. Polarization is used as quantum variable.

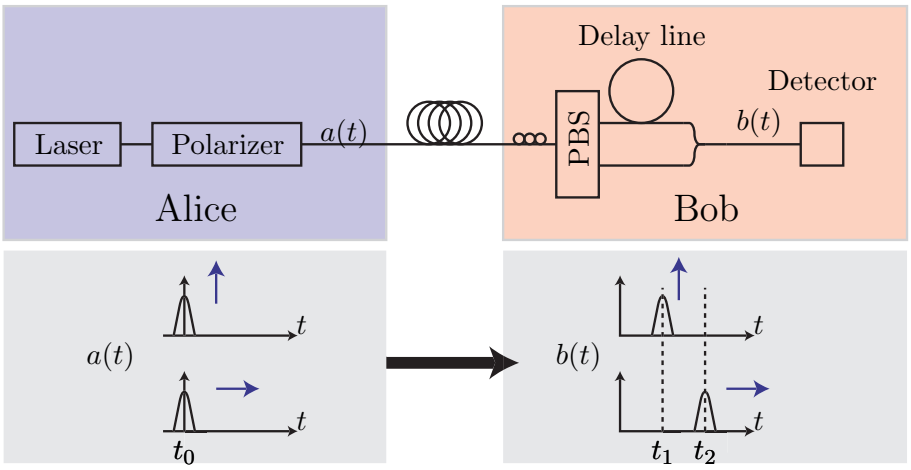


Figure 35: Polarization encoding principle. The pulse arrives at $t = t_1$ if it went through the short arm, and at $t = t_2$ if it went through the long arm. We can then determine the initial polarization state.

The system principle is depicted in Figure 35. Alice uses a fainted laser source and a polarizer to encode the photon polarization state following her random basis and bit choice. Bob uses the two polarization separator outputs, one includes a long arm L. One can delay the pulse on one arm, and determine as a function of arrival time, the initial input polarization.

The first experiment on a deployed fiber was performed in 1995 over a 23km distance [51] between cities of Geneva and Nyon. The chosen wavelength was 1300nm in order to minimize transmission losses, and to use efficient detectors. This experiment used an optical fiber that is, contrary to free space, birefringent where it is difficult to control polarization

variations. An additional polarization control must be included to make this experiment stable in time.

3.1.3 Phase and Information Encoding

The quantum information can be encoded on the phase of a photon with respect to pulses. Information encoding with phase may be interpreted as the use of a very large interferometer where one can slightly modify the optical path length, and thus, modify the pulse phase on one arm, Φ_1, and Φ_2 , see Figure 36

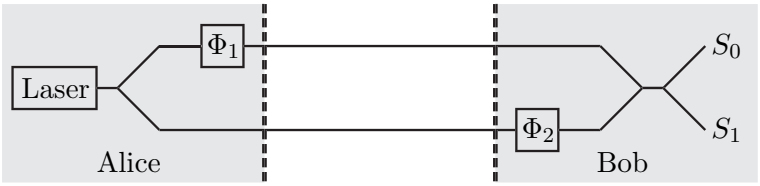


Figure 36: Phase Encoding with BB84 protocol.

When both phases Φ_1 and Φ_2 are identical, i.e., $\Phi_1 = \Phi_2$, the resulting interferences from this long interferometer are constructive and light is detected on detector S_0. When the phase difference is π, $|\Phi_2 - \Phi_1| = \pi$, light is observed on the second mode interferometer output S_1. When the phase difference is $\pm\pi/2$, $|\Phi_2 - \Phi_1| = \pm\pi/2$, energy is evenly split on both modes, that is half on S_0 and half on S_1.

For the BB84 protocol, we consider the following four phase values for Φ_1: $\Phi_1 = 0$: $|u_0\rangle$, $\Phi_1 = \pi$: $|u_1\rangle$, $\Phi_1 = +\pi/2$: $|v_0\rangle$, $\Phi_1 = -\pi/2$: $|v_1\rangle$. Bob's measurement on one of either bases is determined by phase Φ_2: either $\Phi_2 = 0$ for basis U, or $\Phi_2 = +\pi/2$ for basis V. When the initial state is chosen in a different basis, the phase difference is $\pm\pi/2$ and the energy is split over the two interferometer outputs. When an incident photon must be detected with a phase difference $|\Delta\Phi| = \pm\pi/2$, detection occurs randomly on either output. There is finally an equivalence table to implement BB84 protocol with phase, see Table 5.

Table 5: Phase Equivalence Table.

Basis	U: $\Phi_2 = 0$	V: $\Phi_2 = \pi/2$
States	$\|u_0\rangle$: $\Phi_1 = 0$	$\|v_0\rangle$: $\Phi_1 = +\pi/2$
	$\|u_1\rangle$: $\Phi_1 = \pi$	$\|v_1\rangle$: $\Phi_1 = -\pi/2$

The phase encoding hurdle is to keep the length of two interferometer arms constant.

The light paths must be identical, i.e., the relative variations are very small compared with the optical wavelength. All practical systems develop methods to compensate possible physical length variations.

3.1.4 Phase Encoding Experiments

3.1.4.1 Time Separated Signals

In 1993, Townsend, Rarity, and Tapser proposed a quantum cryptography system using photon phase [66, 65], that combines the links of the very long interferometer into two interferometers with shorter arms to reduce length variation sensitivity.

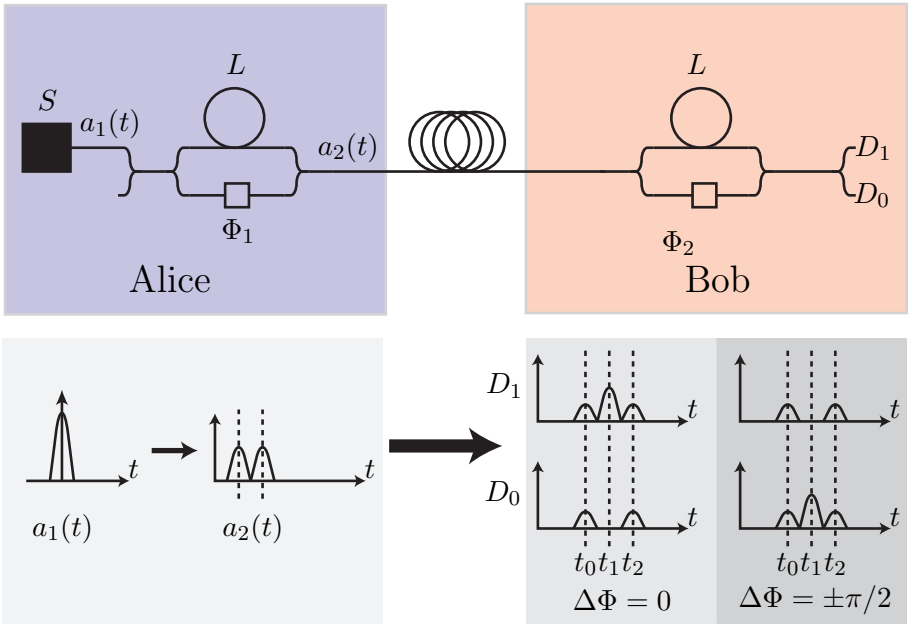


Figure 37: Phase Encoding Principle. Two pulses exit Alice apparatus, and interfere on Bob's side.

The schematic in Figure 37 uses a single fiber between Alice and Bob. Alice generated a pulse from a laser source S. It is split by a first beam splitter toward two arms, where the first one, the long arm L_1 includes an extra fiber length to delay the pulse. The short arm includes an optical phase shifter Φ_1. The two recombined pulses are time separated. These pulses are split again at Bob's input, whose interferometer includes also a long and a short arm, to recombine pulse and induce interference. The resulting interference outcomes on output 0 or 1 is a function of the phase difference $\Delta\Phi = \Phi_2 - \Phi_1$.

The quality of the interferences relies on the fact that both long arms from Alice's and Bob's interferometers have exactly identical optical paths, which is hard to maintain over a long period of time.

In 2002, Inoue, Waks, and Yamamoto developed [42, 41] a system with only one interferometer described in Figure 38. Alice generates light pulses at a given rate f_0. These pulses are modulated with a phase modulator before being injected through the optical fiber. Bob uses an unbalanced interferometer, which optical path difference L corresponding exactly to delay $\tau_0 = 1/f_0$. Then, each photon interferes with the next pulse, making impossible for an eavesdropper to extract only one pulse. This system presents the advantage to use a fainted laser source as photon source while being resistant to a Receive & Resend attack.

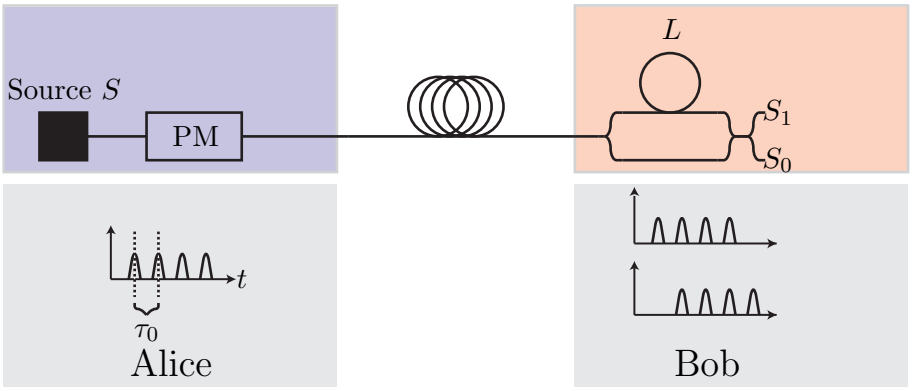


Figure 38: Phase Difference Shift System. Pulses are sent at f_0 frequency where time τ_0 corresponds to the propagation over the distance L. Then, each pulse interferes with the following and previous pulses.

3.1.4.2 The Plug&Play System

The quantum key distribution system called Plug&Play was developed initially by Stucki *et al.* in 1993 [63]. It uses phase. It is able to compensate for component characteristics fluctuation over time. Optical pulses make a round trip between Alice and Bob. The problem of maintaining the interferometer arm length is then alleviated. Information is encoded in the phase between two optical time separated pulses, see Figure 39.

While Alice is the source of the transmission, the 1550nm wavelength laser is located on Bob's side. He sends two pulses through the fiber to Alice. She applies a Φ_1 phase shift on the second pulse with a phase modulator PM_A and reflects the pulse to Bob with a Faraday

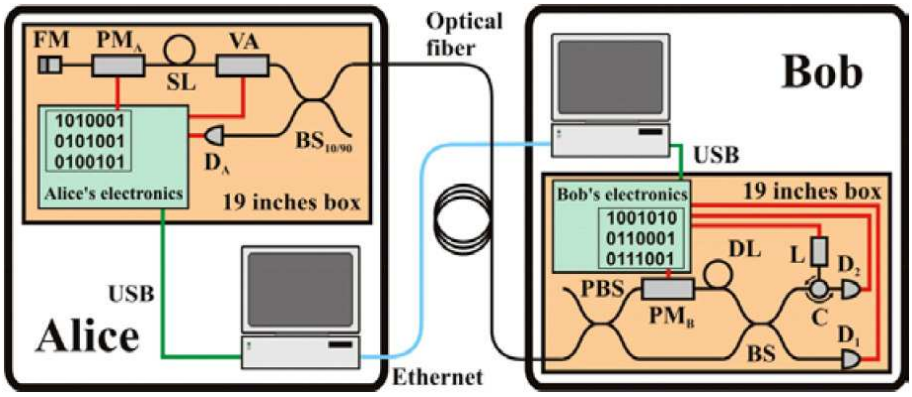


Figure 39: Plug&Play QKD System Principle. [63].

mirror FM. The pulse is received by Bob, who applies a Φ_2 phase shift on one arm. Then, the pulses interfere in the beam splitter. This interference is detected on two sensors D_1 and D_2. The system auto-compensates the optical path variations as each pulse travels on the same path back and forth. This system has been tested on a fiber going under the Geneva lake, over 67km between Lausanne, Geneva, and Nyon cities. This principle has been used by a startup company IdQuantique. It packaged into a standard telecom rack as a final commercial product.

3.1.4.3 Frequency Separated Signals

Another way to encode phase is to use two different frequencies. Duraffourg showed that the relative phase difference between two frequency separated pulses that may interfere to recover initial phase of transmitted signal [49]. The principle was then developed to complete a quantum key transmission using the BB84 protocol [22, 48, 35]. This setup is the one we will study in detail in this thesis.

All presented methods are very sensitive to mechanical variations and require specific setups to maintain stability over time. In optical transmission systems developed on large scale, many components designed for phase modulation are produced. These may be used for a quantum key distribution setup where coding is performed with frequency separated signals.

One may also notice that quantum cryptography is entering the industrialization era. Some companies, still at the startup stage, are attempting to provide security systems

including quantum cryptography tools. Current products are available from IdQuantique, Switzerland, MagiQ Technologies, US, QinetiQ, UK, for which the implementation of QKD principles are kept unpublished. Other companies such as Toshiba, BBN, and HP are deploying QKD links.

3.2 Single Side Band (SSB) Encoding

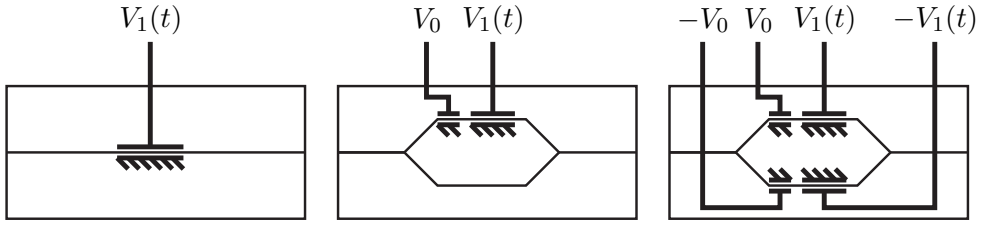
3.2.1 Frequency Encoding

3.2.1.1 Frequency Domain and Modulation

The quantum variable chosen to encode states is the relative phase between two waves with very close frequencies. We consider the phase difference between a pulse with a given optical frequency and its side bands generated by modulation. The use of the frequency domain enables a narrow temporal spread. The information is sent at multiple frequencies inside a single pulse. Time and spectral domain are efficiently used. Coding in frequency domain is easily accessible with standard telecom modulators whose performance is well known and described thereafter.

3.2.1.2 Modulators and Frequency Manipulation

A telecom modulator relies on the electro-optic effect of material such as Lithium Niobate substrate ($LiNbO_3$) whose optical index varies with a applied voltage perpendicularly to the optical path. By creating electrodes on a wave guide in such material, one can change the optical path. The magnetic wave field describing the optical wave in the wave guide varies. Modulators affecting frequencies are from three types: phase modulators, standard Mach-Zhender interferometers (MZI), and push-pull MZIs, see Figure 40.



(a) Phase Modulator (b) Standard MZI Modulator (c) Push-Pull MZI Modulator

Figure 40: Phase Modulator and Mach-Zhender Modulators Architectures.

Phase Modulator In phase modulators, see Figure 40(a), when the modulation voltage is applied to electrodes, $V_1(t) = m\sin(\Omega t + \Phi)$, it modifies the optical index as a function of time at frequency Ω. The resulting modulation function introduces a sinusoidal wave phase shift which is:

$$T_{\text{Phase}} = e^{KV_1(t)} = e^{jKm\sin(\Omega t+\Phi)}, \tag{54}$$

where K is a coefficient that is electro-optic material dependent, and m is the modulation depth, proportional to the amplitude $V_1(t)$.

The Jacobi-Anger expansion leads to $e^{jA\sin\varphi} = \sum_{n=-\infty}^{+\infty} j^n J_n(A)e^{jn\varphi}$ where J_n is the first kind Bessel function to the order n. Equation (54) expands into:

$$T_{\text{Phase}} = \sum_{n=-\infty}^{+\infty} j^n J_n(m)e^{jn(\Omega t+\Phi)}. \tag{55}$$

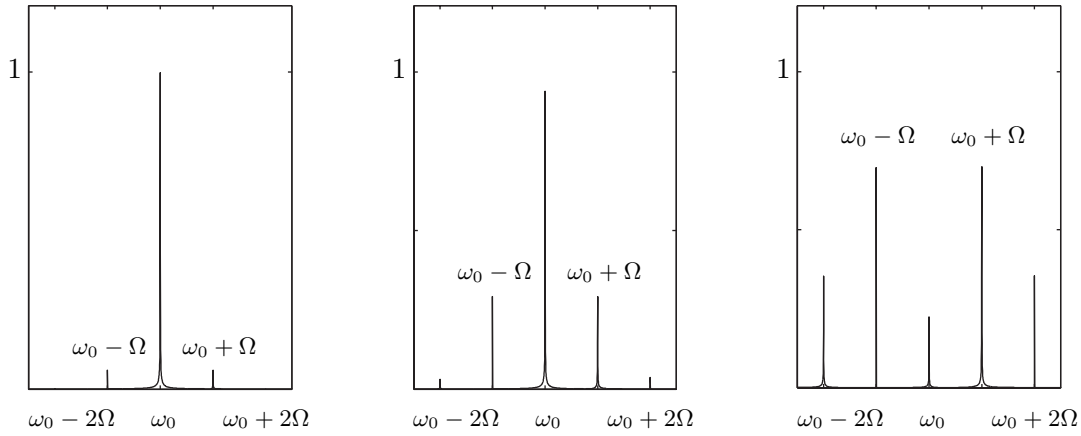
The modulator transforms a single frequency signal $E(t) = E_0 e^{j\omega_0 t}$ into a signal with multiple harmonic frequencies $\omega_0 + n\Omega$. Considering that $m \ll 1$, only first order in m development remains. This signal contains then only two harmonics:

$$\begin{aligned} T_{\text{Phase}}E(t) &= E_0 e^{j\omega_0 t}\sum_{n=-\infty}^{+\infty} j^n J_n(m)e^{jn(\Omega t+\Phi)} \\ &= E_0 e^{j\omega_0 t}\left(J_0(m) + jJ_1(m)e^{j(\Omega t+\Phi)} - jJ_{-1}(m)e^{-j(\Omega t+\Phi)}\right) \\ &= E_0 e^{j\omega_0 t} + E_0\frac{m}{2}e^{j((\omega_0+\Omega)t+\Phi)} - E_0\frac{m}{2}e^{j((\omega_0-\Omega)t-\Phi)} \end{aligned} \tag{56}$$

Figure 41 shows spectra amplitudes at phase modulator output for different value of m. From Figure 41(b) and 41(c), the central peak at frequency ω_0 no longer has a normalized amplitude of one. Peaks at second harmonics frequencies $\omega_0 \pm 2\Omega$ appear then. When modulation depth m has become too important to be considered as "low", the first order in m expansion from Equation (56) is not longer sufficient. It is necessary to consider the second order in m:

$$\begin{aligned} T_{\text{Phase}}E(t) = E_0(1-\frac{m^2}{4})e^{j\omega_0 t} + E_0\frac{m}{2}e^{j((\omega_0+\Omega)t+\Phi)} - E_0\frac{m}{2}e^{j((\omega_0-\Omega)t-\Phi)} \\ - E_0\frac{m^2}{8}e^{j((\omega_0+2\Omega)t+2\Phi)} - E_0\frac{m^2}{8}e^{j((\omega_0-2\Omega)t-2\Phi)}. \end{aligned} \tag{57}$$

Standard MZI For standard MZIs, the structure includes two arms, one of them including two electrodes, see Figure 40. A first continuous voltage V_0 creates a constant phase



(a) Low amplitude modulation depth $m = 0.1$

(b) Average amplitude modulation depth $m = 0.5$

(c) High amplitude modulation depth $m = 2$

Figure 41: Spectrum amplitude at the phase modulator output for a normalized input. Figures are drawn with different modulation depth values m.

shift $e^{jKV_0} = e^{j\Psi}$. A second sinusoidal voltage $V_1(t)$ creates an additional variation of the optical path $e^{jKV_1(t)}$. The resulting modulation transfer function is:

$$T_{\text{MZI}} = \frac{1 + e^{j\Psi} e^{jm\sin(\Omega t + \Phi)}}{2}. \tag{58}$$

For $m \ll 1$, the modulator output may be expressed at the first order in m:

$$\begin{aligned} T_{\text{MZI}} E(t) &= E_0 e^{j\omega_0 t} \frac{1 + e^{j\Psi} e^{jm\sin(\Omega t + \Phi)}}{2} \\ &= E_0 \frac{1 + e^{j\Psi}}{2} e^{j\omega_0 t} + jE_0 \frac{m}{4} e^{j((\omega_0 + \Omega)t + \Phi + \Psi)} - jE_0 \frac{m}{4} e^{j((\omega_0 - \Omega)t - \Phi + \Psi)}. \end{aligned} \tag{59}$$

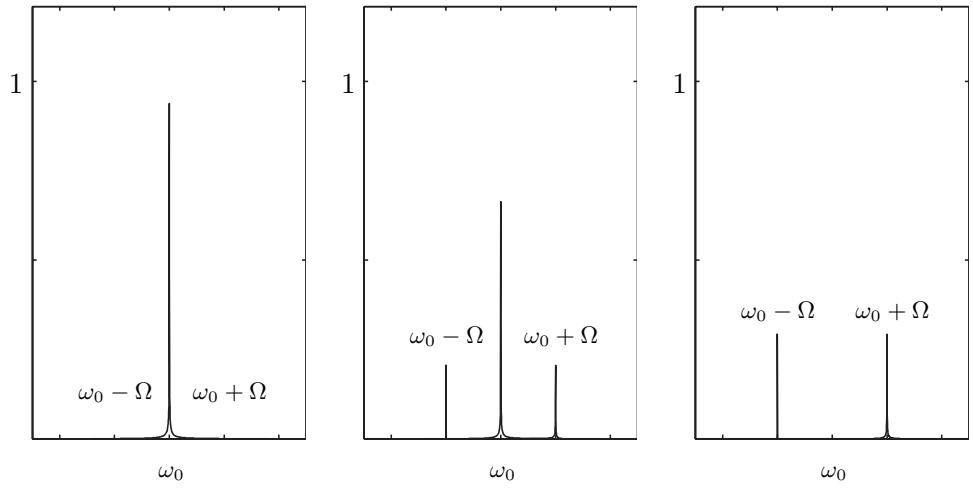
The central peak amplitude is now dependent on Ψ.

Push-pull MZI Finally, the push-pull MZI modulator spreads the modulation voltage on both arms: positive voltage on the first one, and inverse voltage on the second one, see

Figure 40(c). The modulator output is then at first order in m:

$$\begin{aligned} T_{\text{MZI push-pull}}E(t) &= E_0 e^{j\omega_0 t}\frac{e^{-j\Psi}e^{-jm\sin(\Omega t+\Phi)}+e^{j\Psi}e^{jm\sin(\Omega t+\Phi)}}{2} \\ &= E_0\frac{e^{-j\Psi}+e^{j\Psi}}{2}e^{j\omega_0 t} \\ &\quad + E_0\frac{m(e^{j\Psi}-e^{-j\Psi})}{4}e^{j((\omega_0+\Omega)t+\Phi)} - E_0\frac{m(e^{j\Psi}-e^{-j\Psi})}{4}e^{j((\omega_0-\Omega)t-\Phi)} \\ &= E_0\cos(\Psi)e^{j\omega_0 t} \\ &\quad + jE_0\frac{m\sin(\Psi)}{2}e^{j((\omega_0+\Omega)t+\Phi)} - jE_0\frac{m\sin(\Psi)}{2}e^{j((\omega_0-\Omega)t-\Phi)}. \end{aligned} \tag{60}$$

The push-pull MZI output signal spectrum as a function of bias voltage is shown Figure 42.



(a) $\Psi = 0$ (b) $\Psi = \pi/4$ (c) $\Psi = \pi/2$

Figure 42: Push-pull MZI output spectrum amplitude for different bias voltage values Ψ.

Phase modulators or MZIs are effective components to control the time delay (or phase delay) between signals at different frequencies. Their characteristics are very well known, as they are used in standard telecommunication networks.

3.2.2 SSB Principle and Double Modulation

As described in the previous part, information encoding with relative phase between two signals at different frequencies makes an efficient use of the time domain. The system developed at GTL-CNRS Telecom uses the relative phase between the central peak and the

modulated side bands. The modulation scheme permits the detection of a single side band (SSB). The basic principle was first described by Duraffourg [22] on Figure 43.

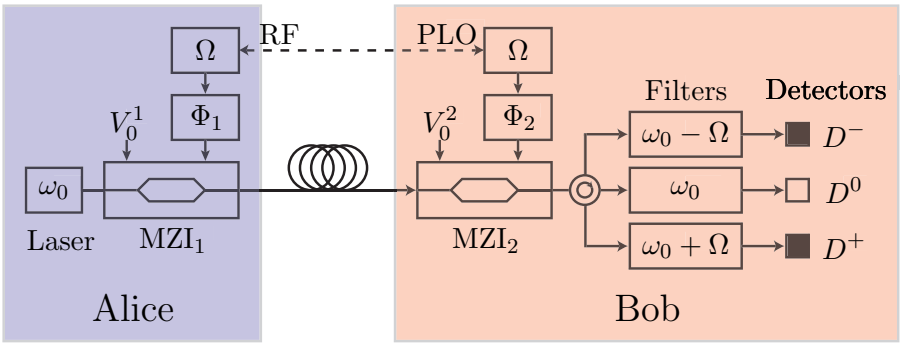


Figure 43: SSB Modulation Scheme Principle.

3.2.2.1 System Architecture Description

On Alice's side, the system includes an optical line made of a laser diode generating optical pulses at frequency ω_0 and a modulator MZI_1. The fiber link between Alice and Bob is then connected on Bob's side to a modulator MZI_2. The optical signal is filtered to extract three frequencies $\omega_0 - \Omega$, ω_0, and $\omega_0 + \Omega$. Three amplitude detectors D^-, D^0, and D^+ measure the signal amplitudes $i_{\omega_0-\Omega}$, i_{ω_0} et $i_{\omega_0+\Omega}$ respectively.

An electrical line controls the modulators and includes an RF oscillator at frequency Ω. An electric shifter adjusts the phase Φ_1 of the signal applied to modulator MZI_1. Bob has also an oscillator at frequency Ω synchronized on Alice's one and a second phase shifter to set phase Φ_2 of the signal applied to modulator MZI_2.

3.2.2.2 System Operating Principle

A laser diode generates an optical field $E_1(t) = E_0 e^{j\omega_0 t}$. This signal is modulated through MZI_1 and driven by a sinusoidal voltage $V_1(t) = m\sin(\Omega t + \Phi_1)$, with $m \ll 1$, and a continuous polarization voltage V_0^1 that creates a constant phase shift on one arm $e^{j\Psi_1}$. The optical field at Alice's modulator output MZI_1 is:

$$\begin{aligned} E_{\text{Alice}} &= E_1(t)\frac{1 + e^{j(\Psi_1 + V_1(t))}}{2}, \\ &= E_0 e^{\omega_0 t}\frac{1 + e^{j\Psi_1}e^{jm\sin(\Omega t + \Phi_1)}}{2}. \end{aligned} \tag{61}$$

The signal is transmitted along the fiber. Upon arrival, Bob modulates the received signal with MZI_2 with bias Ψ_2 and sinusoidal signal $V_2(t)$:

$$\begin{aligned} E_{\mathrm{Bob}} &= E_{\mathrm{Alice}}(t)\frac{1+e^{j(\Psi_2+V_2(t))}}{2} = E_1(t)\frac{1+e^{j(\Psi_1+V_1(t))}}{2}\cdot\frac{1+e^{j(\Psi_2+V_2(t))}}{2} \\ &= \frac{E_0 e^{j\omega_0 t}}{4}\left(1+e^{j\Psi_1}e^{jV_1(t)}+e^{j\Psi_2}e^{jV_2(t)}+e^{j\Psi_1+\Psi_2}e^{j(V_1(t)+V_2(t))}\right). \end{aligned} \tag{62}$$

Using the first order expansion of $e^{jV_1(t)}$ and $e^{jV_2(t)}$, Equation (62) becomes:

$$\begin{aligned} E_{\mathrm{Bob}} &= \frac{E_0 e^{j\omega_0 t}}{4}\Big[1+e^{j\Psi_1}\left(1+j\frac{m}{2}e^{j(\Omega t+\Phi_1)}-j\frac{m}{2}e^{-j(\Omega t+\Phi_1)}\right) \\ &\quad + e^{j\Psi_2}\left(1+j\frac{m}{2}e^{j(\Omega t+\Phi_2)}-j\frac{m}{2}e^{-j(\Omega t+\Phi_2)}\right) \\ &\quad + e^{j(\Psi_1+\Psi_2)}\left(1+j\frac{m}{2}e^{j(\Omega t+\Phi_1)}-j\frac{m}{2}e^{-j(\Omega t+\Phi_1)}\right)\left(1+j\frac{m}{2}e^{j(\Omega t+\Phi_2)}-j\frac{m}{2}e^{-j(\Omega t+\Phi_2)}\right)\Big] \\ &= \frac{E_0 e^{j\omega_0 t}}{4}\Big[1+e^{j\Psi_1}+e^{j\Psi_2}+e^{j(\Psi_1+\Psi_2)} \\ &\quad + j\frac{m}{2}e^{j\Omega t}\left(e^{j\Psi_1}e^{j\Phi_1}+e^{j\Psi_2}e^{j\Phi_2}+e^{j(\Psi_1+\Psi_2)}\left(e^{j\Phi_1}+e^{j\Phi_2}\right)\right) \\ &\quad - j\frac{m}{2}e^{-j\Omega t}\left(e^{j\Psi_1}e^{-j\Phi_1}+e^{j\Psi_2}e^{-j\Phi_2}+e^{j(\Psi_1+\Psi_2)}\left(e^{-j\Phi_1}+e^{-j\Phi_2}\right)\right)\Big]. \end{aligned} \tag{63}$$

The side band intensity at frequency $\omega_0+\Omega$, $i_{\omega_0+\Omega}$ is:

$$\begin{aligned} i_{\omega_0+\Omega} &= \left\|\frac{m}{2}\left(e^{j\Psi_1}e^{j\Phi_1}+e^{j\Psi_2}e^{j\Phi_2}+e^{j(\Psi_1+\Psi_2)}\left(e^{j\Phi_1}+e^{j\Phi_2}\right)\right)\right\|^2 \\ &= \frac{m^2}{4}\left(e^{j\Psi_1}e^{j\Phi_1}+e^{j\Psi_2}e^{j\Phi_2}+e^{j(\Psi_1+\Psi_2)}e^{j\Phi_1}+e^{j(\Psi_1+\Psi_2)}e^{j\Phi_2}\right) \\ &\qquad \times\left(e^{-j\Psi_1}e^{-j\Phi_1}+e^{-j\Psi_2}e^{-j\Phi_2}+e^{j(-\Psi_1-\Psi_2)}e^{-j\Phi_1}+e^{j(-\Psi_1-\Psi_2)}e^{-j\Phi_2}\right) \\ &= \frac{m^2}{4}\Big(4+e^{j(\Delta\Phi+\Delta\Psi)}+e^{j(-\Delta\Phi-\Delta\Psi)}+e^{j\Psi_1}+e^{-j\Psi_1}+e^{j\Psi_2}+e^{-j\Psi_2} \\ &\qquad +e^{j(-\Psi_1-\Delta\Phi)}+e^{j(\Psi_1+\Delta\Phi)}+e^{j(-\Psi_2+\Delta\Phi)}+e^{j(\Psi_2-\Delta\Phi)}+e^{j\Delta\Phi}+e^{-j\Delta\Phi}\Big) \\ &= m^2\Big[1+\cos\left(\frac{\Delta\Psi}{2}\right)\cos\left(\Delta\Phi+\frac{\Delta\Psi}{2}\right) \\ &\qquad +\cos\left(\frac{\Delta\Psi}{2}\right)\cos\Psi'+\cos\Psi'\cos\left(\Delta\Phi+\frac{\Delta\Psi}{2}\right)\Big], \end{aligned} \tag{64}$$

where $\Delta\Phi=\Phi_2-\Phi_1$, $\Delta\Psi=\Psi_2-\Psi_1$ and $\Psi'=\dfrac{\Psi_1+\Psi_2}{2}$.

The side band intensity at frequency $\omega_0 - \Omega$ is computed similarly:

$$\begin{aligned} i_{\omega_0-\Omega} &= \left\| \frac{m}{2} \left(e^{j\Psi_1} e^{-j\Phi_1} + e^{j\Psi_2} e^{-j\Phi_2} + e^{j(\Psi_1+\Psi_2)} \left(e^{-j\Phi_1} + e^{-j\Phi_2} \right) \right) \right\|^2 \\ &= m^2 \left[1 + \cos\left(\frac{\Delta\Psi}{2}\right) \cos\left(\Delta\Phi - \frac{\Delta\Psi}{2}\right) \right. \\ &\qquad \left. + \cos\left(\frac{\Delta\Psi}{2}\right) \cos\Psi' + \cos\Psi' \cos\left(\Delta\Phi - \frac{\Delta\Psi}{2}\right) \right]. \end{aligned} \tag{65}$$

If the biases comply with the following conditions:

$$\frac{\Delta\Psi}{2} = \frac{\Psi_2 - \Psi_1}{2} = \frac{\pi}{2} + k\pi \Rightarrow \cos\left(\frac{\Delta\Psi}{2}\right) = 0 \tag{66}$$

$$\Psi' = \frac{\Psi_2 + \Psi_1}{2} = 0 + k'\pi \Rightarrow \cos\left(\Psi'\right) = \pm 1 \tag{67}$$

Both possible solutions in $[0, 2\pi]$ are:

$$\Psi_1 = +\frac{\pi}{2} \quad \text{and} \quad \Psi_2 = -\frac{\pi}{2} \qquad \text{Solution 1} \tag{68}$$

$$\Psi_1 = -\frac{\pi}{2} \quad \text{and} \quad \Psi_2 = +\frac{\pi}{2} \qquad \text{Solution 2} \tag{69}$$

Both solutions are equivalent to exchange both Alice's and Bob's modulators. The central peak intensity i_{ω_0} is:

$$i_{\omega_0} = \left\| \frac{E_0}{4}(1 + j - j + 1) \right\|^2 = \frac{E_0^2}{4}. \tag{70}$$

Equation (64) and Equation (65) becomes:

$$i_{\omega_0+\Omega} = \frac{E_0^2}{16} m^2 (1 + \cos(\Delta\Phi)) = i_{\omega_0} \frac{m^2}{2} \cos^2\left(\frac{\Delta\Phi}{2}\right) \tag{71}$$

$$i_{\omega_0-\Omega} = \frac{E_0^2}{16} m^2 (1 - \cos(\Delta\Phi)) = i_{\omega_0} \frac{m^2}{2} \sin^2\left(\frac{\Delta\Phi}{2}\right) \tag{72}$$

One can notice that when the relative phase difference $\Delta\Phi$ is 0 or π, the energy outside central peak is located on one side band and one only. When $\Delta\Phi = \pm\pi/2$, the energy is evenly split on both sidebands, see Figure 44.

3.2.2.3 SSB Scheme with Push-Pull MZI and Phase Modulator.

The above configuration may also be achieved with a single push-pull modulator with bias Ψ and sinusoidal signal $\sim \Omega t + \Phi_1$ on a phase modulator with modulation $\sin \Omega t + \Phi_2$. The obtained optical wave field is:

$$\begin{aligned} E_{\text{Bob}} = E_0 e^{j\omega_0 t} \Big[&\cos(\Psi) + \left(\frac{m}{2} \cos\Psi \, e^{j\Phi_2} + j\frac{m}{2} \sin\Psi \, e^{j\Phi_1} \right) \\ &- \left(\frac{m}{2} \cos\Psi \, e^{-j\Phi_2} + j\frac{m}{2} \sin\Psi \, e^{-j\Phi_1} \right) \Big]. \end{aligned} \tag{73}$$

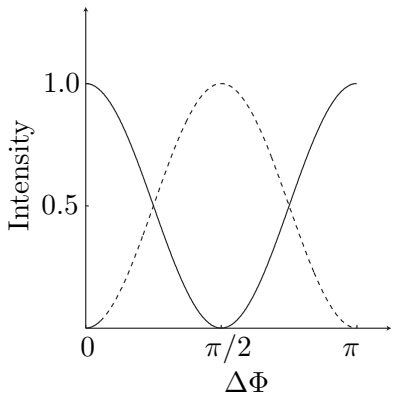


Figure 44: Intensities measured on sidebands at frequencies $\omega_0 - \Omega$ (dotted line) and $\omega_0 + \Omega$ (plain line), as a function of relative phase difference $\Delta\Phi$.

If we consider $\Psi = \pi/4$, i.e., $\cos\Psi = \sin\Psi$, Equation (73) becomes

$$\begin{aligned} E_{\text{Bob}} &= \frac{\sqrt{2}E_0 e^{\omega_0 t}}{2}\left[1 + \frac{m}{2}\left(e^{j\Phi_2} + je^{j\Phi_1}\right) - \frac{m}{2}\left(e^{-j\Phi_2} + je^{-j\Phi_1}\right)\right] \\ &= \frac{\sqrt{2}E_0 e^{\omega_0 t}}{2}\left[1 + me^{j\left(\frac{\Phi_1' + \Phi_2}{2}\right)}\cos(\Delta\Phi) + me^{j\left(-\frac{\Phi_1' + \Phi_2}{2}\right)}\sin(\Delta\Phi)\right]. \end{aligned} \tag{74}$$

where $\Phi_1' = \Phi_1 + \dfrac{\pi}{2}$ and $\Delta\Phi = \dfrac{\Phi_2' - \Phi_1}{2}$. The sidebands intensities are in phase opposition:

$$i_{\omega_0+\Omega} = i_{\omega_0} m^2 \cos^2\left(\frac{\Delta\Phi}{2}\right), \tag{75}$$

$$i_{\omega_0-\Omega} = i_{\omega_0} m^2 \sin^2\left(\frac{\Delta\Phi}{2}\right). \tag{76}$$

One can observe exactly these same intensity for $\cos\Psi = \pm\sin\Psi$, i.e.,

$$\Psi \in \left\{\frac{\pi}{4}, \frac{3\pi}{4}, \frac{5\pi}{4}, \frac{7\pi}{4}\right\}. \tag{77}$$

As only one condition on the bias voltage of the push-pull modulator is required, the implementation of such a system is easier.

3.2.3 System Behavior Summary

The system behavior and working points are summarized below:

Sidebands energy:

$$i_{\omega_0+\Omega} = \alpha m^2 \cos^2\left(\frac{\Delta\Phi}{2}\right)$$
$$i_{\omega_0-\Omega} = \alpha m^2 \sin^2\left(\frac{\Delta\Phi}{2}\right),$$

where α is a constant.

Condition on the modulator bias voltages:

Two MZIs	MZI and Phase Modulator
$\begin{cases}\Psi_1 = -\pi/2 \\ \Psi_2 = +\pi/2\end{cases}$ or $\begin{cases}\Psi_1 = +\pi/2 \\ \Psi_2 = -\pi/2\end{cases}$	$\Psi = \pi/4$, or $\Psi = 3\pi/4$, or $\Psi = 5\pi/4$, or $\Psi = 7\pi/4$

3.2.4 Quantum Interpretation of the SSB Scheme

When the pulse energy is strongly lowered, the above behavior remains unchanged. Fainted light pulses are modeled with coherent states (Glauber states) or quasi-classical states.

The classical description of the modulation scheme stays valid for quantum states. It is possible to build an equivalence between variable elements and quantum variables, measurements and projections, that matches the BB84 protocol description in Section 1.2.1.

In quantum regime, the photon detection probability is proportional to the incoming signal energy. When $\Delta\Phi = 0$ or $\Delta\Phi = \pi$, only one detector D^+ or D^- may have an incoming photon. In the same manner, when $\Delta\Phi = \pm\pi/2$, the photon is randomly detected on one or the other detector. Thus, it is possible to implement the BB84 protocol [7] as described by Duraffourg [22].

The initial bias phase Φ_1 Alice's modulation electric signal corresponds to the initial choice of the quantum state to be sent. Bob's electric signal bias phase Φ_2 corresponds to the basis of the quantum measurement. The quantum projection corresponds to the frequency filtering and detection to measure the state on a given basis.

The states from basis B_1, $|u_0\rangle$ and $|u_1\rangle$, correspond to Alice's initial phases 0 and π. The states from basis B_2, $|v_0\rangle$ and $|v_1\rangle$, correspond to phase state $+\pi/2$ and $-\pi/2$. We

have then:

$$\begin{aligned} \Phi_1 = 0 \mapsto |u_0\rangle \qquad \Phi_1 = \pi/2 \mapsto |v_0\rangle \\ \Phi_1 = \pi \mapsto |u_1\rangle \quad \Phi_1 = -\pi/2 \mapsto |v_1\rangle \end{aligned} \tag{78}$$

In the same manner, Bob's measurement with a given basis may be matched to Bob's modulator phase Φ_2. The measurement is then a rotation of the state sent by Alice along with the matrix $M_\Phi = \begin{pmatrix} \cos(\Phi/2) & \sin(\Phi/2) \\ -\sin(\Phi/2) & \cos(\Phi/2) \end{pmatrix}$.

$$\begin{aligned} \Phi_2 = 0 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \Phi_2 = +\pi/2 \mapsto \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \\ \Phi_2 = \pi \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \Phi_2 = -\pi/2 \mapsto \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}. \end{aligned} \tag{79}$$

Finally, the detection is a projection on basis vectors $|u_0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|u_1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Projections on vectors $|u_0\rangle$ and $|u_1\rangle$ correspond to detections on D^+ et D^-:

$$\begin{aligned} D^+ \mapsto \langle u_0| \\ D^- \mapsto \langle u_1| \end{aligned} \tag{80}$$

It is then possible to implement the BB84 protocol as described in Section 1.2.1. First, Alice prepares one pulse among four possible states and sends the pulse modulated with phase Φ_1 randomly chosen in $E_\Phi = \{0, \pi/2\,\pi, -\pi/2\}$. Second, Bob receives the pulse and remodulates it with a phase Φ_2 chosen in $E'_\Phi = \{0, \pi/2\}$. Finally, Bob uses two detectors D^+ et D^-. The BB84 protocol may then be summarized in Table 6.

3.3 Single Side Pulse (SSP) Encoding

Phase encoding with time separated pulses is used in many quantum key distribution systems [66, 42, 63]. Inoue also introduced a three arm modulator for QKD [41]. The use of time-energy vs. frequency-time entanglement for quantum information communication makes the time filtering easier vs. frequency filtering.

To conserve the advantage of the *strong reference* in the SSB, that makes it resistant to the PNS attack, I introduce a transposition of the SSB in the time domain called single side

Table 6: BB84 Protocol with SSB System. Black disks • show a full detection probability, and white disks ∘ show a half probability for each detector.

Alice's Bit	Alice Φ_1	Bob Φ_2	Difference $\Delta\Phi$	D^+	D^-	Shared Bit
1	0	0	0		•	1
		$+\pi/2$	$+\pi/2$	∘	∘	-
0	π	0	π	•		0
		$+\pi/2$	$-\pi/2$	∘	∘	-
1	$+\pi/2$	0	$-\pi/2$	∘	∘	-
		$+\pi/2$	0		•	1
0	$-\pi/2$	0	$+\pi/2$	∘	∘	-
		$+\pi/2$	π	•		0

pulse (SSP) detection scheme. As for the SSB scheme with frequencies, the SSP scheme relies on multiple time separated pulses to the sides of a main strong energy pulse. A three pulse sequence encodes the information in the phase difference between the main powerful pulse and the other two weak pulses.

The secure capacity of the quantum channel can be viewed the same way as for a classical channel. The transposition into of the SSB scheme in the time domain to give the SSP scheme is motivated by the need of increased throughput for a given channel. With both SSB and SSP, it is possible to multiplexed then and use coding such as Quadrature Amplitude Modulation[1], or QAM [54], to increase throughput and get closer to the capacity.

3.3.1 Time Domain Modulation

The SSB uses MZIs to encode information. It creates sidebands along the main peak. It is not possible to create directly a side pulse that would be *before* the main pulse. So we can take advantage of propagation time and delay the main pulse.

We propose to use a three arm interferometer to match the MZI behavior in the time domain, see Figure 45. It allows to introduce two side pulses aside the main pulse. The second and third lines include delay lines of length L and $2L$. An additional bias phase Ψ is applied to set the operating point. Finally, an extra phase Φ is applied in opposite sign to encode information.

[1]Quadrature amplitude modulation is a big name for a relatively simply technique. It is simply a combination of amplitude modulation and phase shift keying.

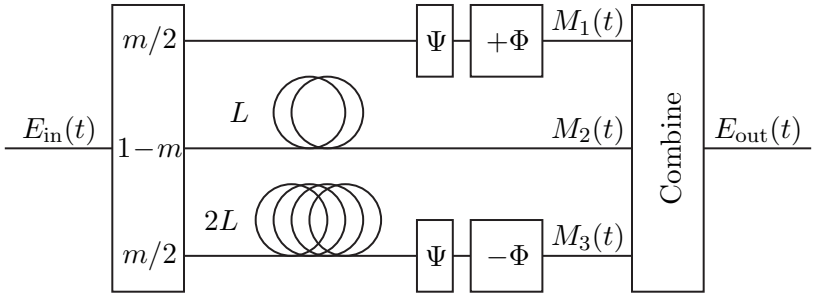


Figure 45: Single Side Pulse Interferometer Principle.

When a single frequency laser pulse $\delta(t)E_0e^{j\omega_0 t}$ is sent to the interferometer, see Figure 46(a), the following signal incomes the modulator:

$$E_{\text{in}}(t) = \delta(t'_1)E_0e^{j\omega_0(t'_1)}, \tag{81}$$

with $t'_1 = t - \tau'_1$. Then the output signal is:

$$\begin{aligned} E_{\text{out}} =& \frac{m}{2}E_{\text{in}}(t-\tau'_1)e^{j\Psi}e^{+j\Phi} + (1-m)E_{\text{in}}(t-\tau'_1-\tau_L) \\ &+ \frac{m}{2}E_{\text{in}}(t-\tau'_1-2\tau_L)e^{j\Psi}e^{-j\Phi} \\ =& \frac{m}{2}\delta(t'_1)E_0e^{j\omega_0 t'_1}e^{j\Psi}e^{+j\Phi} + (1-m)\delta(t_1)E_0e^{j\omega_0 t_1} \\ &+ \frac{m}{2}\delta(t^*_1)E_0e^{j\omega_0 t^*_1}e^{j\Psi}e^{-j\Phi} \end{aligned} \tag{82}$$

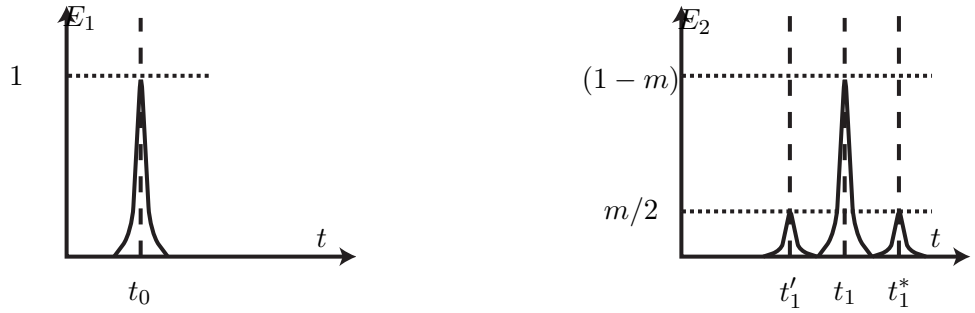
where τ_L is the delay induced by L, $t_1 = t - \tau'_1 - \tau_L$, and $t^*_1 = t - \tau'_1 - 2\tau_L$.

When the recombined signals, two side pulses are created, see Figure 46(b). Their relative phase difference to the main pulse is Φ and $-\Phi$, respectively, and is the information encoded in the signal.

This modulation Figure 46(b), and the Equation (82) are the exact same as in the frequency domain with Figure 41(b) and Equation (59). The delay τ_L introduced by the extra length of the modulator corresponds to the modulation frequency Ω in the frequency domain.

3.3.2 SSP Modulation Scheme and BB84 Protocol

The complete system includes an interferometer on Alice's side and another on Bob's side with initial bias phase set to Ψ_1 and Ψ_2, see Figure 47. After two interferences, the resulting pulse sequence amplitude is shown in Figure 46(b). Second harmonic side pulses are



(a) Single Pulse. (b) Three Pulses Sequence.

Figure 46: Pulse sequence bearing the quantum information. E_1 is the initial laser signal amplitude envelope, E_2 is the pulse sequence signal amplitude envelope of Alice's output, and E_3 is the signal envelope after a second modulation.

negligible, as $m \ll 1$. We may proceed to a first order approximation.

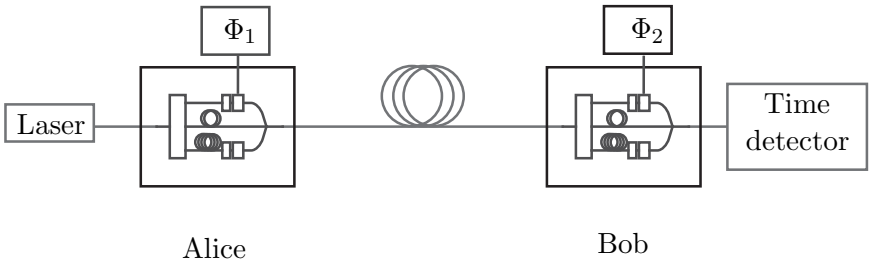


Figure 47: SSP Principle

They system presents the same constraints as Equation (66) and Equation (67) on the operating points Ψ_1 and Ψ_2. Alice and Bob set their operating point with $\Psi_1 = \pi/4$ and $\Psi_2 = -\pi/4$.

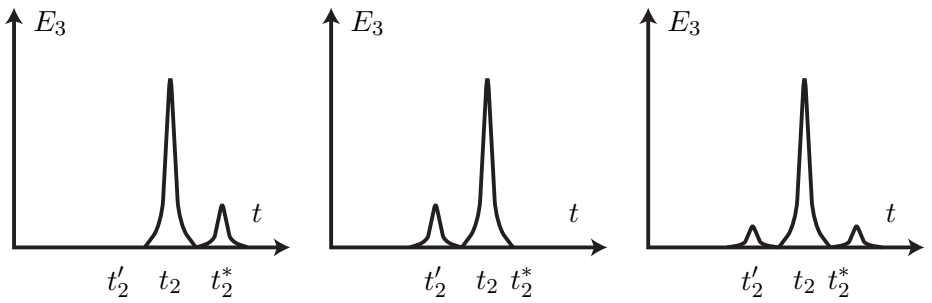
The resulting side pulses amplitude i'_{δ_2} and $i^*_{\delta_2}$ can be expressed with a first order approximation :

$$i'_{\delta_2} = i_{\delta_2} \frac{m^2}{2} \cos^2\left(\frac{\Delta\Phi}{2}\right), \tag{83}$$

$$i^*_{\delta_2} = i_{\delta_2} \frac{m^2}{2} \sin^2\left(\frac{\Delta\Phi}{2}\right), \tag{84}$$

where i_{δ_2} is the amplitude of the central pulse and $\Delta\Phi = \Phi_2 - \Phi_1$ is the phase difference between Alice's and Bob's command signal, see Figure 48. The detection of the side pulses is performed by measuring the photon arrival time compared to the main pulse arrival time.

One big advantage of the SSP system over the SSB system is the low sensibility to



(a) Signal E_3 for $\Delta\Phi = \pi$. (b) Signal E_3 for $\Delta\Phi = 0$. (c) Signal E_3 with $\Delta\Phi = \pm\pi/2$.

Figure 48: Single side pulse (SSP) modulation time plots for different relative phase difference $\Delta\Phi$.

propagation compare to the SSB system. For the SSB system, multiple frequency signal is traveling on the same fiber. Thus, their relative phase is changing along with light path fluctuations. The SSP system in insensitive to this effect as the pulse stream is at the same optical frequency. The remaining constraint for accurate interference is to keep the delay line L constant.

The energy level is lowered to obtain less than photon level energy in total energy in the sidebands. This benefits from the quantum properties, especially the non cloning theorem and the non orthogonality of all encoded states.

3.3.3 Quantum Interpretation of the SSP Scheme

When the energy is strongly lowered, the above behavior remains unchanged. Fainted light pulses are modeled with Coherent states (Glauber states) or quasi-classical states.

As the classical description remains and the amplitudes of side pulses are in phase opposition, it is possible to implement the BB84 protocol the same way as described in [35], see Table 7.

As for the SSB scheme, there is a correspondence between the system variable and the qubit manipulation used in the BB84 protocol. The correspondence for the initial phases Φ_1 and the initial basis and state choice $|u_0\rangle$, $|u_1\rangle$, $|v_0\rangle$, or $|v_1\rangle$ is the same as for Equation (78). The measurements are also viewed with a matrix format $M_\Phi = \begin{pmatrix} \cos(\Phi/2) & \sin(\Phi/2) \\ -\sin(\Phi/2) & \cos(\Phi/2) \end{pmatrix}$ as for Equation (79).

Table 7: BB84 Protocol with SSP interference scheme. The black disks are for 100% pulse detection, nothing for no detection, and white disks for unknown detection on either the front (t_2^*) or the back (t_2') side pulse.

Alice			Bob				
Bit	Basis	Φ_1	Φ_2	$\Delta\Phi$	t_2^*	t_2'	Bit Shared
0	B_1	0	0	0		•	0
			$\pi/2$	$\pi/2$	○	○	
	B_2	$\pi/2$	0	0		•	0
			$\pi/2$	$\pi/2$	○	○	
1	B_1	π	0	π	•		1
			$\pi/2$	$-\pi/2$	○	○	
	B_2	$-\pi/2$	0	π	•		1
			$\pi/2$	$-\pi/2$	○	○	

Finally, the detection is a projection on basis vectors $|u_0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|u_1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Projection on vectors $|u_0\rangle$ and $|u_1\rangle$ to the detection on time slots t_2' and t_2^*:

$$\begin{aligned} t_2' &\mapsto \langle u_0| \\ t_2^* &\mapsto \langle u_1| \end{aligned} \tag{85}$$

3.4 Multiplexing of SSB and SSP Techniques

As the SSP and SSB schemes rely on the time and frequency domains, we can implement both encoding at the same time.

3.4.1 Multiplexing and Demultiplexing Structures

The channel is split in two where each SSB and SSP modulators are used to encode the information, and the lines are then recombined, see Figure 50(a). In order to add up the energy of both central peak, a phase delay Φ_m is added on one arm. The equation of the outgoing signal is:

$$E_{\text{out}} = \frac{E_{\text{SSB}} + e^{j\Phi_m} \cdot E_{\text{SSB}}}{2}, \tag{86}$$

The resulting signal shows two side bands and two side pulses, see Figure 49. These two pairs are separated and independent. The traveling wave carries information on the relative

phase difference between the main peak/pulse and side bands in the frequency domain and side pulses in the time domain.

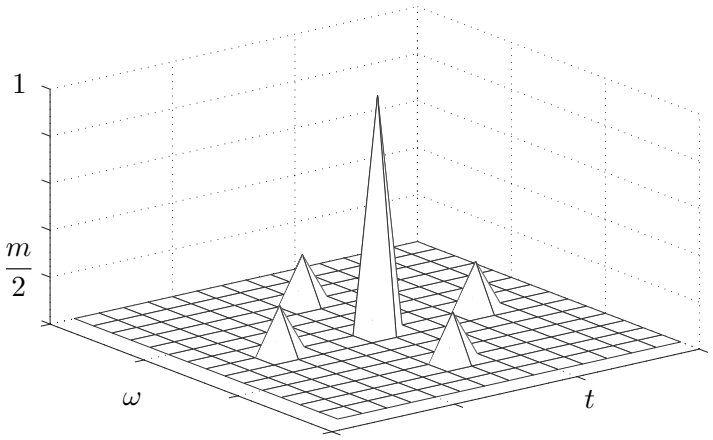
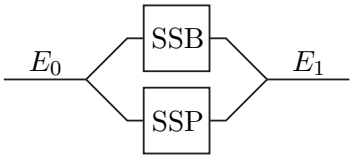
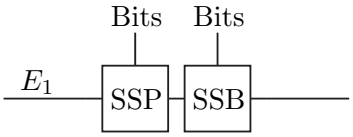


Figure 49: Energy as a function of time and frequency.



(a) Multiplexing of both SSB and SSP



(b) Demultiplexing to recover information

Figure 50: Multiplexing encoding principle of both SSB and SSP on the same channel

For demultiplexing, Bob uses first an MZI to recover the information encoded in the frequency domain with the SSB technique. Then, the pulse is sent through a SSP time modulator to recover the information encoded in the time domain, see Figure 50(b).

3.4.2 Enhanced Throughput

After filtering and measurement, it is possible to extract the information from both the SSB and the SSP encoding techniques. Alice and Bob share twice the information as they would have with only the SSB or the SSP technique. The secure bit rate, i.e., the secure information that is sent and share between the emitter and the receiver in one pulse, is then doubled.

3.5 BB84 Protocol with Reference Security with a Fainted Laser

The BB84 protocol security relies mostly on the use of single photon sources. The modulation technique relies on pulses whose sidebands behave like a multiphoton source that is highly attenuated. Each pulse includes a signal that is use as a reference for phase. In this section, we describe that this strong pulse may be utilized as a strong reference [40] as described in Section 2.3.2.

This signal at frequency ω_0 may be considered as a reference when the two following conditions are fulfilled:

1. Reference must always be detected with the signal.
2. Reference must be linked with the signal. It should not be possible to have a reference signal without information signal.

Condition (1) is obviously fulfilled for any relative phase difference $\Delta\Phi$ as the central peak is always present in the frequency domain. Condition (2) requires more specific attention. It is necessary to check that the eavesdropper cannot create a signal with the reference and no information signal, i.e., a signal that includes the central peak and no sideband once Bob's remodulates the signal. We call such signal a *zero-photon* signal.

Matrix expression of frequency modulation. At our operating conditions, MZI modulators have a linear behavior, thus, it is possible to apply linear algebra to model their behavior. We will work in the vector spaces of frequencies $\omega_0 + k\Omega$, that is the central frequency ω_0 and all harmonics separated by Ω from the central frequency. Then, a vector $\begin{pmatrix} \dots & x_2 & x_1 & x_0 & x_{-1} & x_{-2} & \dots \end{pmatrix}^{\mathrm{T}}$ represents the signal amplitude at frequencies $\dots, \omega_0 - 2\Omega, \omega_0 - \Omega, \omega_0, \omega_0 + \Omega, \omega_0 + 2\Omega, \dots$.

The first order approximation of an MZI modulation function is:

$$T_{\mathrm{MZI}}E(t) = E_0\frac{1+e^{j\Psi}}{2}e^{j\omega_0 t} + jE_0\frac{m}{4}e^{j((\omega_0+\Omega)t+\Phi+\Psi)} - jE_0\frac{m}{4}e^{j((\omega_0-\Omega)t-\Phi+\Psi)}. \qquad (87)$$

It is possible to express the equation with a matrix form:

$$\frac{1}{4}\begin{pmatrix} jme^{j(\Phi+\Psi)} \\ 2(1+e^{j\Psi}) \\ -jme^{j(-\Phi+\Psi)} \end{pmatrix} \cdot \begin{pmatrix} x_0 \end{pmatrix} = \begin{pmatrix} y_1 \\ y_0 \\ y_{-1} \end{pmatrix}. \tag{88}$$

The MZI behavior does not depend on the central optical peak frequency. As the modulator function is linear, one can compute the matrix for a three input signal for example:

$$\frac{1}{4}\begin{pmatrix} jme^{j(\Phi+\Psi)} & 0 & 0 \\ 2(1+e^{j\Psi}) & jme^{j(\Phi+\Psi)} & 0 \\ -jme^{j(-\Phi+\Psi)} & 2(1+e^{j\Psi}) & jme^{j(\Phi+\Psi)} \\ 0 & -jme^{j(-\Phi+\Psi)} & 2(1+e^{j\Psi}) \\ 0 & 0 & -jme^{j(-\Phi+\Psi)} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_0 \\ x_{-1} \end{pmatrix} = \begin{pmatrix} y_2 \\ y_1 \\ y_0 \\ y_{-1} \\ y_{-2} \end{pmatrix}. \tag{89}$$

Each output y_k depends on the value of three input signals x_{k-1}, x_k, et x_{k+1}. We can also express the output value:

$$y_k = \frac{jme^{j(\Phi+\Psi)}}{4}x_{k-1} + \frac{1+e^{j\Psi}}{2}x_k - \frac{jme^{j(-\Phi+\Psi)}}{4}x_{k+1}. \tag{90}$$

3.5.0.1 Building a zero-photon signal with an MZI

In this section, we determine when the eavesdropper is able to generate a zero-photon signal. We are constructing a signal such that Bob, after modulation, will always detect with the reference, but will never detect any signal on the sidebands. We assume that Alice uses a modulation depth m that is very low. Bob will apply a modulation with low modulation depth to generate destructive interferences on first order sidebands. Eve generates a signal a central frequency ω_0 with harmonics at frequencies $\omega_0 + k\Omega$ of form:

$$E_{\text{Eve}} = \sum_{k=-\infty}^{+\infty} x_k e^{j(\omega_0+k\Omega)t}. \tag{91}$$

The signal, after Bob's modulation, must not include any energy at frequency $\omega_0 + \Omega$ and $\omega_0 - \Omega$ when Bob uses phase 0 and $\pi/2$. Moreover, central peak amplitude must be of equal amplitude as it would be without Eve's presence. These conditions may be translated

into matrix form:

$$A \cdot \begin{pmatrix} x_2 \\ x_1 \\ x_0 \\ x_{-1} \\ x_{-2} \end{pmatrix} = \begin{pmatrix} -\frac{m}{4} & \frac{1-j}{2} & \frac{m}{4} & 0 & 0 \\ \frac{jm}{4} & \frac{1-j}{2} & \frac{jm}{4} & 0 & 0 \\ 0 & -\frac{m}{4} & \frac{1-j}{2} & \frac{m}{4} & 0 \\ 0 & \frac{jm}{4} & \frac{1-j}{2} & \frac{jm}{4} & 0 \\ 0 & 0 & -\frac{m}{4} & \frac{1-j}{2} & \frac{m}{4} \\ 0 & 0 & \frac{jm}{4} & \frac{1-j}{2} & \frac{jm}{4} \end{pmatrix} \cdot \begin{pmatrix} x_2 \\ x_1 \\ x_0 \\ x_{-1} \\ x_{-2} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \tag{92}$$

This predetermined system has five unknowns and six equations. It is overdetermined and can be solved with the generalized inverse:

$$A^H \cdot A \cdot \begin{pmatrix} x_2 \\ x_1 \\ x_0 \\ x_{-1} \\ x_{-2} \end{pmatrix} = A^H \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \tag{93}$$

$$\begin{pmatrix} m^2 & -2m & 0 & 0 & 0 \\ -2m & 8+m^2 & -2m(1-j) & 0 & 0 \\ 0 & -2m(1+j) & 8+2m^2 & -2m(1-j) & 0 \\ 0 & 0 & -2m(1+j) & 8m^2 & 2m \\ 0 & 0 & 0 & -2jm & m^2 \end{pmatrix} \cdot \begin{pmatrix} x_2 \\ x_1 \\ x_0 \\ x_{-1} \\ x_{-2} \end{pmatrix} = \begin{pmatrix} 0 \\ 2m(-1-j) \\ 8(1+j) \\ 2m(1-j) \\ 0 \end{pmatrix}$$

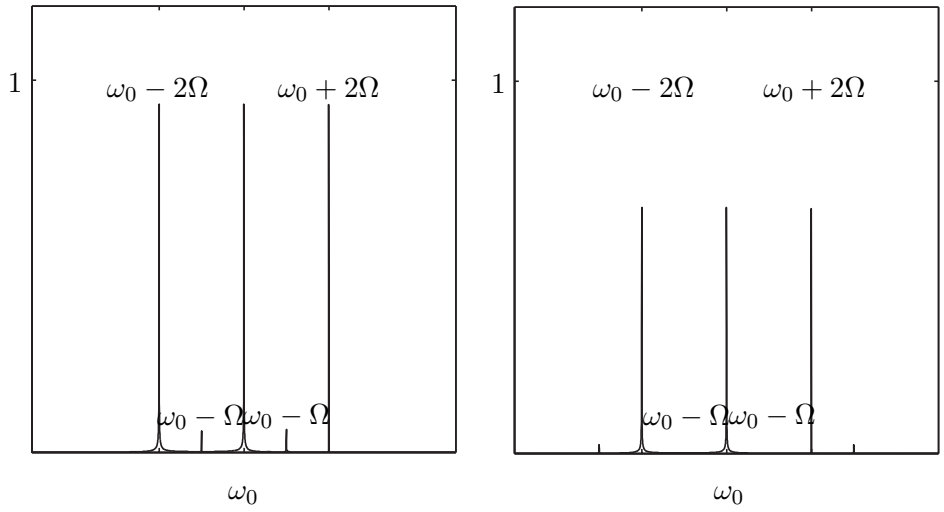
The matrix $A^H A$ is of rank 5, it is then possible to invert it to obtain matrix $(A^H A)^{-1}$. The solution is then:

$$\begin{pmatrix} x_2 \\ x_1 \\ x_0 \\ x_{-1} \\ x_{-2} \end{pmatrix} = (A^H A)^{-1} A^H \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \frac{2(1-j)}{-j(4+jm^2)} \begin{pmatrix} 2j \\ -jm \\ 2 \\ m \\ -2j \end{pmatrix} \tag{94}$$

The remaining error of the solution compared to initial conditions is indeed zero:

$$\mathcal{E} = \left\| \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} - A \begin{pmatrix} x_2 \\ x_1 \\ x_0 \\ x_{-1} \\ x_{-2} \end{pmatrix} \right\| = 0 \tag{95}$$

This solution is presented in Figure 51(a) and the corresponding Bob's output in Figure 51(b). One can notice that the solution is perfect; Bob will detect exactly 0 on both sidebands.



(a) *Zero-photon* signal generated by Eve.

(b) Bob's modulator output. The spectrum is identical for $\Phi = 0$ and $\Phi = \pi/2$.

Figure 51: *Zero-Photon* Signal

Under this condition, the protocol does not really have a reference. In the following section we will show how to prevent Eve to be able to generate a zero-photon signal.

3.5.1 Blocking a Zero-Photon Signal

3.5.1.1 Blocking with higher harmonics detectors

One can observe the signal at Bob's modulator output includes second order harmonics $\omega_0 \pm 2\Omega$ of same amplitude order as the central peak. One solution to prevent Eve from building such a signal is to add two additional detectors at frequencies $\omega_0 - 2\Omega$ and $\omega_0 + 2\Omega$.

When Bob detects some energy at these frequencies, Eve may be in the channel. Alice and Bob should stop communication.

Eve may use further orders harmonics, i.e., 3, 4, or further if necessary to eliminate second harmonics on Bob's side. This generates the following condition:

$$A \cdot \begin{pmatrix} x_3 \\ x_2 \\ x_1 \\ x_0 \\ x_{-1} \\ x_{-2} \\ x_{-3} \end{pmatrix} = \begin{pmatrix} -\frac{m}{4} & \frac{1-j}{2} & \frac{m}{4} & 0 & 0 & 0 & 0 \\ -\frac{jm}{4} & \frac{1-j}{2} & \frac{jm}{4} & 0 & 0 & 0 & 0 \\ 0 & -\frac{m}{4} & \frac{1-j}{2} & \frac{m}{4} & 0 & 0 & 0 \\ 0 & -\frac{jm}{4} & \frac{1-j}{2} & \frac{jm}{4} & 0 & 0 & 0 \\ 0 & 0 & -\frac{m}{4} & \frac{1-j}{2} & \frac{m}{4} & 0 & 0 \\ 0 & 0 & -\frac{jm}{4} & \frac{1-j}{2} & \frac{jm}{4} & 0 & 0 \\ 0 & 0 & 0 & -\frac{m}{4} & \frac{1-j}{2} & \frac{m}{4} & 0 \\ 0 & 0 & 0 & -\frac{jm}{4} & \frac{1-j}{2} & \frac{jm}{4} & 0 \\ 0 & 0 & 0 & 0 & -\frac{m}{4} & \frac{1-j}{2} & \frac{m}{4} \\ 0 & 0 & 0 & 0 & -\frac{jm}{4} & \frac{1-j}{2} & \frac{jm}{4} \end{pmatrix} \cdot \begin{pmatrix} x_3 \\ x_2 \\ x_1 \\ x_0 \\ x_{-1} \\ x_{-2} \\ x_{-3} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad (96)$$

In the same manner, one can solve the system $A^H AX = A^H B$. The inverse $(A^H A)^{-1}$ exists and the least square solution is:

$$\begin{pmatrix} x_3 \\ x_2 \\ x_1 \\ x_0 \\ x_{-1} \\ x_{-2} \\ x_{-3} \end{pmatrix} = \frac{1+j}{8} \begin{pmatrix} -2jm(1+j) \\ -m^2(1+j) \\ -2jm \\ 8 \\ 2m \\ m^2(1+j) \\ 2jm(1+j) \end{pmatrix} \quad (97)$$

Bob's detection error is in first order in m:

$$\mathcal{E} = \left\| \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} - A \begin{pmatrix} x_3 \\ x_2 \\ x_1 \\ x_0 \\ x_{-1} \\ x_{-2} \\ x_{-3} \end{pmatrix} \right\| \approx \frac{1}{4} \left\| \begin{pmatrix} 0 \\ 0 \\ m \\ -m \\ 0 \\ 0 \\ -jm \\ jm \\ 0 \\ 0 \end{pmatrix} \right\| \approx m. \tag{98}$$

The best signal generated by Eve leaves a remaining component of order $m/4$ on each first order sideband. This will create errors and Eve will be revealed. To have third order harmonics contributing to cancel signal at frequencies $\omega_0 \pm 2\Omega$, Eve must consider the expansion in m^2 of Bob's modulator. The MZI modulation function matrix is:

$$M = \begin{pmatrix} \alpha_2 e^{-2j\Phi_2} & -\alpha_1 e^{-j\Phi_2} & \alpha_0 & \alpha_1 e^{j\Phi_2} & \alpha_2 e^{2j\Phi_2} & 0 & 0 \\ 0 & \alpha_2 e^{-2j\Phi_2} & -\alpha_1 e^{-j\Phi_2} & \alpha_0 & \alpha_1 e^{j\Phi_2} & \alpha_2 e^{2j\Phi_2} & 0 \\ 0 & 0 & \alpha_2 e^{-2j\Phi_2} & -\alpha_1 e^{-j\Phi_2} & \alpha_0 & \alpha_1 e^{j\Phi_2} & \alpha_2 e^{2j\Phi_2} \end{pmatrix} \tag{99}$$

where $\alpha_2 = \dfrac{-jm^2}{8}, \alpha_1 = \dfrac{-m}{4}, \alpha_0 = \dfrac{4 - 4j + jm^2}{8}$.

Then, the modulator output is:

$$M \cdot \begin{pmatrix} x_3 \\ x_2 \\ x_1 \\ x_0 \\ x_{-1} \\ x_{-2} \\ x_{-3} \end{pmatrix}_{\text{Input}} = A \begin{pmatrix} x_1 \\ x_0 \\ x_{-1} \end{pmatrix}_{\text{Output}} \tag{100}$$

The Equation (96) is at second order in m becomes:

$$\begin{pmatrix} \alpha_2 & -\alpha_1 & \alpha_0 & \alpha_1 & \alpha_2 & 0 & 0 & 0 & 0 \\ -\alpha_2 & -j\alpha_1 & \alpha_0 & j\alpha_1 & -\alpha_2 & 0 & 0 & 0 & 0 \\ 0 & \alpha_2 & -\alpha_1 & \alpha_0 & \alpha_1 & \alpha_2 & 0 & 0 & 0 \\ 0 & -\alpha_2 & -j\alpha_1 & \alpha_0 & j\alpha_1 & -\alpha_2 & 0 & 0 & 0 \\ 0 & 0 & \alpha_2 & -\alpha_1 & \alpha_0 & \alpha_1 & \alpha_2 & 0 & 0 \\ 0 & 0 & -\alpha_2 & -j\alpha_1 & \alpha_0 & j\alpha_1 & -\alpha_2 & 0 & 0 \\ 0 & 0 & 0 & \alpha_2 & -\alpha_1 & \alpha_0 & \alpha_1 & \alpha_2 & 0 \\ 0 & 0 & 0 & -\alpha_2 & -j\alpha_1 & \alpha_0 & j\alpha_1 & -\alpha_2 & 0 \\ 0 & 0 & 0 & 0 & \alpha_2 & -\alpha_1 & \alpha_0 & \alpha_1 & \alpha_2 \\ 0 & 0 & 0 & 0 & -\alpha_2 & -j\alpha_1 & \alpha_0 & j\alpha_1 & -\alpha_2 \end{pmatrix} \begin{pmatrix} x_4 \\ x_3 \\ x_2 \\ x_1 \\ x_0 \\ x_{-1} \\ x_{-2} \\ x_{-3} \\ x_{-4} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \tag{101}$$

where $\alpha_2 = \dfrac{-jm^2}{8}, \alpha_1^0 = \dfrac{-m}{4}$, and $\alpha_0 = \dfrac{4 - 4j + jm^2}{8}$.

In the same manner, one can solve the $A^H AX = A^H B$ system.

One can compute the inverse $(A^H A)^{-1}$ and find the solution X, an approximation being:

$$\begin{pmatrix} x_4 \\ x_3 \\ x_2 \\ x_1 \\ x_0 \\ x_{-1} \\ x_{-2} \\ x_{-3} \\ x_{-4} \end{pmatrix} \approx \begin{pmatrix} \dfrac{1}{m^2}(1.23 + 1.84j) \\ \dfrac{1}{m}(0.31 - 1.54j) \\ 0 \\ m(0.27 - 0.34j) \\ 1 + j \\ m(0.34 + 0.27j) \\ 0 \\ \dfrac{1}{m}(-1.54 - 0.31j) \\ \dfrac{1}{m^2}(1.23 + 1.84j) \end{pmatrix}. \tag{102}$$

The spectrum amplitude of the signal generated by Eve is shown in Figure 52.

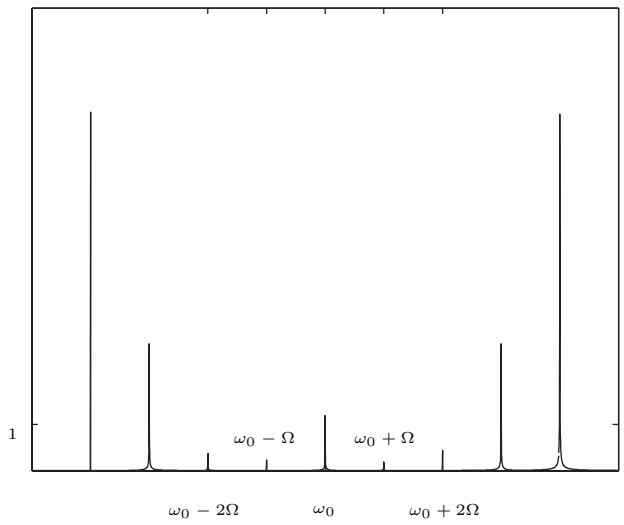


Figure 52: Eve's signal spectrum amplitude for $m = 0.5$.

This solution gives a zero error:

$$\mathcal{E} = \left\| \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} - A \begin{pmatrix} x_4 \\ x_3 \\ x_2 \\ x_1 \\ x_0 \\ x_{-1} \\ x_{-2} \\ x_{-3} \\ x_{-4} \end{pmatrix} \right\| = 0 \tag{103}$$

Bob obtains a signal where second order harmonics are zero for $\phi_2 \in \{0, \pi/2\}$. Although, it is important to notice that Eve needs to generate a signal with amplitude $1/m^2$, that may then be very high for a very small m. Bob may perform an energy measurement on the whole signal, thus detecting the high average energy generated by Eve.

Bob has the possibility to implement additional detectors on higher harmonics, making it harder for Eve the generation of a *zero-photon* signal. She has to use even higher harmonics, thus producing a very high energy signal that is then easily detectable by Bob.

3.5.1.2 Enhancing the BB84 Protocol

A more elegant solution than adding detectors on harmonics is to take advantage of the easy structure of the SSB system. It is easy for Bob to modify the modulator phase values to π or $-\pi/2$ without modifying the system. Choosing $\Phi_2 = \pi$ is equivalent for Bob to choose phase $\Phi_2 = 0$ and swapping the sideband signal. Then, bit 0 may be detected on the detector D^-, and bit 1 on detector D^+ respectively. Table 6 is modified into Table 8.

Table 8: Enhance BB84 protocol for SSB system.

Alice's Bit	Alice Φ_1	Bob Φ_2	Difference $\Delta\Phi$	D^+	D^-	Shared Bit
1	0	0	0		•	1
		$+\pi/2$	$+\pi/2$	∘	∘	-
		π	π	∘	∘	-
		$-\pi/2$	$-\pi/2$	•		1
0	π	0	π	•		0
		$+\pi/2$	$-\pi/2$	∘	∘	-
		π	0		•	0
		$-\pi/2$	$+\pi/2$	∘	∘	-
1	$+\pi/2$	0	$-\pi/2$	∘	∘	-
		$+\pi/2$	0		•	1
		π	$+\pi/2$	∘	∘	-
		$-\pi/2$	π	•		1
0	$-\pi/2$	0	$+\pi/2$	∘	∘	-
		$+\pi/2$	π	•		0
		π	$-\pi/2$	∘	∘	-
		$-\pi/2$	0		•	0

This enhanced BB84 protocol version enables communication with only one detector, as detector D^+ and D^- are able to detect each bit 0 and 1.

Bob's choice for Φ_2 is among four possible values 0, $+\pi/2$, π, and $-\pi/2$. The number of constraints for Eve to generate a zero-photon pulse doubles. Then, to cancel the quantum information first harmonics, as Bob chooses among four phase values, Eve has to zero eight

conditions on sidebands. The matrix form becomes:

$$A \cdot \begin{pmatrix} x_2 \\ x_1 \\ x_0 \\ x_{-1} \\ x_{-2} \end{pmatrix} = \begin{pmatrix} -\frac{m}{4} & \frac{1-j}{2} & \frac{m}{4} & 0 & 0 \\ \frac{jm}{4} & \frac{1-j}{2} & \frac{jm}{4} & 0 & 0 \\ \frac{m}{4} & \frac{1-j}{2} & -\frac{m}{4} & 0 & 0 \\ -\frac{jm}{4} & \frac{1-j}{2} & -\frac{jm}{4} & 0 & 0 \\ 0 & -\frac{m}{4} & \frac{1-j}{2} & \frac{m}{4} & 0 \\ 0 & \frac{jm}{4} & \frac{1-j}{2} & \frac{jm}{4} & 0 \\ 0 & \frac{m}{4} & \frac{1-j}{2} & -\frac{m}{4} & 0 \\ 0 & -\frac{jm}{4} & \frac{1-j}{2} & -\frac{jm}{4} & 0 \\ 0 & 0 & -\frac{m}{4} & \frac{1-j}{2} & \frac{m}{4} \\ 0 & 0 & \frac{jm}{4} & \frac{1-j}{2} & \frac{jm}{4} \\ 0 & 0 & \frac{m}{4} & \frac{1-j}{2} & -\frac{m}{4} \\ 0 & 0 & -\frac{jm}{4} & \frac{1-j}{2} & -\frac{jm}{4} \end{pmatrix} \cdot \begin{pmatrix} x_2 \\ x_1 \\ x_0 \\ x_{-1} \\ x_{-2} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}. \tag{104}$$

One computes the matrix $A^H A$ that is:

$$A^H A = \begin{pmatrix} \frac{m^2}{4} & 0 & 0 & 0 & 0 \\ 0 & \frac{8+m^2}{4} & 0 & 0 & 0 \\ 0 & 0 & \frac{4+m^2}{2} & 0 & 0 \\ 0 & 0 & 0 & \frac{8+m^2}{4} & 0 \\ 0 & 0 & 0 & 0 & \frac{m^2}{4} \end{pmatrix} \tag{105}$$

This matrix $A^H A$ is easily inverted:

$$(A^H A)^{-1} = \begin{pmatrix} \frac{4}{m^2} & 0 & 0 & 0 & 0 \\ 0 & \frac{4}{8+m^2} & 0 & 0 & 0 \\ 0 & 0 & \frac{2}{4+m^2} & 0 & 0 \\ 0 & 0 & 0 & \frac{4}{8+m^2} & 0 \\ 0 & 0 & 0 & 0 & \frac{4}{m^2} \end{pmatrix} \tag{106}$$

The solution X and the error rate are then:

$$\mathcal{E} = \left\| \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} - A \begin{pmatrix} x_2 \\ x_1 \\ x_0 \\ x_{-1} \\ x_{-2} \end{pmatrix} \right\| = \left\| \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} - \frac{1}{m^2+4} \begin{pmatrix} m(1+j) \\ m(-1+j) \\ m(-1-j) \\ m(1-j) \\ 4 \\ 4 \\ 4 \\ m(-1-j) \\ m(-1+j) \\ m(1+j) \\ m(1-j) \end{pmatrix} \right\| = \frac{m(8\sqrt{2}+4m)}{m^2+4}. \quad (107)$$

As previously, a remaining component of order $m/4$ is left on each sidebands, this will create errors for Bob's detection. Eve will be detected. It is then necessary for Eve to proceed with further order harmonics. By using the expansion in m^2 for Bob's modulator, see Equation (99), one can compute the following conditions with matrix form:

$$\begin{pmatrix} \alpha_2 & -\alpha_1 & \alpha_0 & \alpha_{+1} & \alpha_{+2} & 0 & 0 \\ -\alpha_2 & j\alpha_1 & \alpha_0 & j\alpha_{+1} & -\alpha_{+2} & 0 & 0 \\ \alpha_2 & \alpha_1 & \alpha_0 & -\alpha_{+1} & \alpha_{+2} & 0 & 0 \\ -\alpha_2 & -j\alpha_1 & \alpha_0 & -j\alpha_{+1} & -\alpha_{+2} & 0 & 0 \\ 0 & \alpha_2 & -\alpha_1 & \alpha_0 & \alpha_{+1} & \alpha_{+2} & 0 \\ 0 & -\alpha_2 & j\alpha_1 & \alpha_0 & j\alpha_{+1} & -\alpha_{+2} & 0 \\ 0 & \alpha_2 & \alpha_1 & \alpha_0 & -\alpha_{+1} & \alpha_{+2} & 0 \\ 0 & -\alpha_2 & -j\alpha_1 & \alpha_0 & -j\alpha_{+1} & -\alpha_{+2} & 0 \\ 0 & 0 & \alpha_2 & -\alpha_1 & \alpha_0 & \alpha_{+1} & \alpha_{+2} \\ 0 & 0 & -\alpha_2 & j\alpha_1 & \alpha_0 & j\alpha_{+1} & -\alpha_{+2} \\ 0 & 0 & \alpha_2 & \alpha_1 & \alpha_0 & -\alpha_{+1} & \alpha_{+2} \\ 0 & 0 & -\alpha_2 & -j\alpha_1 & \alpha_0 & -j\alpha_{+1} & -\alpha_{+2} \end{pmatrix} \begin{pmatrix} x_3 \\ x_2 \\ x_1 \\ x_0 \\ x_{-1} \\ x_{-2} \\ x_{-3} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad (108)$$

The matrix $A^H A$ is invertible, it is then possible to obtain a least square estimation of the solution:

$$\mathcal{E} = \left\| \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} - A \begin{pmatrix} x_3 \\ x_2 \\ x_1 \\ x_0 \\ x_{-1} \\ x_{-2} \\ x_{-3} \end{pmatrix} \right\| = \left\| \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} - \frac{4 + 4j - jm^2}{2m^4 + 64} \begin{pmatrix} 4m \\ 4jm \\ -4m \\ -4jm \\ 8(1-j) + 2m^2 \\ 8(1-j) + 2m^2 \\ 8(1-j) + 2m^2 \\ 8(1-j) + 2m^2 \\ -4m \\ 4jm \\ 4m \\ -4jm \end{pmatrix} \right\| \approx \frac{1}{4} \begin{pmatrix} m \\ m \\ m \\ m \\ 0 \\ 0 \\ 0 \\ 0 \\ m \\ m \\ m \\ m \end{pmatrix} \tag{109}$$

A $m/4$ component remains on each sideband. In the same manner, any higher harmonics will not be able to eliminate this remain that creates detection errors on Bob's end.

By using four phase values, Bob makes the SSB system resistant against the PNS attack because Eve is not able to create a zero-photon signal without leaving a residual error that leads to false detections on Bob's side. Eve will be revealed during the comparison phase because the key error rate will have increased. Then, as described in Section 2.3.2 and thanks to a strong reference use, Alice is able to use a laser source with an average energy of $\mu = 1$ phton/pulse. Alice and Bob then proceed to a privacy amplification step to eliminate the remaining information known by Eve.

3.5.2 Attenuated Reference with Propagation

As the reference is an optical signal, it is also attenuated. Eve could use this imperfection to increase the amount of information that she may gain. Let us suppose that the strong reference has an initial energy E_{ref}, and is attenuated during transmission with a coefficient $10^{-\frac{\alpha d}{10}}$, where α is the fiber attenuation.

When Bob is at a distance d from Alice such as $10^{-\frac{\alpha d}{10}} \cdot E_{\text{ref}} > 1$, then Bob may detect the reference signal amplitude and then verify that Eve does not create any zero-photon signal.

When the signal energy is less than one photon per pulse, Bob may only perform a statistical analysis on the detected photon over the total pulses. When the average pulse number awaited by Bob is η, Eve may take advantage to generate an optimum signal that generates the least amount of errors, containing exactly one photon in the reference signal over η pulses. The other pulses, $1-\eta$, are blocked. They do not contain any signal. Though, in this case, Bob may notice that he does not receive any reference signal. Moreover, if Eve does not *a priori* know the encoding basis, she will create errors in the bit string shared by Alice and Bob.

For example, if reference amplitude is 0.2 photon per pulse at Bob's detector, Eve creates an optimum signal on 20% of the pulses, and no signal on 80%. Then, Eve generates only 20% of pulses and the overall generated error is only 25%*0.2 = 5% on attacked pulses. Bob will have no information on the remaining bits.

3.6 Conclusion

The SSB system introduced by Duraffourg [22] described in this chapter is a simple quantum key distribution modulation scheme with only two modulators. This modulation may either be implemented with a standard MZI modulator at both the emission and reception sides, or with a push-pull MZI modulator and a phase modulator. This configuration versatility enables a broader flexibility for implementation. The use of phase encoding with multiple frequencies permits less polarization sensitivity to optical fiber birefringence.

The SSP system that we introduced [34] and described in this thesis is built on the same double modulation principle, but in the time domain. A three arm modulator adds two information bearing side pulses to a single input pulse. A double modulation enables the recovery of the information transmitted with the pulses. The BB84 protocol may then be used with this encoding technique.

Both systems may be multiplexed for information encoding in the time and frequency

domains [33]. The throughput is then increases for an identical pulse rate. This system is the first described scheme that uses multiplexing to enhance quantum key distribution secure throughput.

We showed that the addition of an extra detector to the central frequency enables the implementation of the BB84 with reference protocol for both the SSB and SSP schemes [32, 33]. It is impossible for Eve to perform a PNS attack that consists of stealing one photon in multiphoton pulses, and to block single photon pulses. Eve cannot create a zero-photon pulse that Bob would use to detect the reference without detecting the sideband signal. Moreover, Bob may enhance his protocol by using four possible phase states in $\{0, \pi, \pi/2, -\pi/2\}$. The best signal that Eve may generate introduces a remaining energy on both sidebands, which produces a 25% probability to be detected by Bob, and finally a 12.5% error rate on the final key. Thus, Eve may be discovered, as she introduces errors on the transmitted key.

It is possible to implement a prototype with off-the-shelf telecom items such as laser diodes or modulators [35]. The initial average energy at Alice's output may be tuned to one photon per pulse. This is an important gain compared to existing QKD implementations that use a fainted laser. We are going to study more precisely the implementation and performance of this system in the following chapter.

CHAPTER IV

IMPLEMENTATION OF THE SSB SYSTEM WITH REFERENCE

The potential success of a new technology relies on its capacity to be integrated into thinking scheme, but mostly on the way to be easily and efficiently deployed at a decent cost. Then, we have implemented a quantum key distribution system using SSB scheme with standard telecom components. The security and performance in terms of rate and distance are directly influenced by the transmission QBER. We will study in detail how the implementation of the system allowing to have a very low error rate, optimizing then the bit rate, and allowing to guarantee stability over time.

The SSB principle implementation is first described in Section 4.1. Two MZI modulators driven by a HF electric signal allow to obtain signals at frequencies $\omega_0 - \Omega$ and $\omega_0 + \Omega$, where the amplitudes varies in phase opposition, allowing to implement the BB84 protocol. Then, an automatization of the system may be implemented with a computer that allow long encryption keys transmission over long periods of time, see Section 4.2. Then, Section 4.3 presents a system that allows to synchronize the MZI modulations and then to autocompensate any light path fluctuation. In Section 4.4, the implementation of a strong reference detection is described, confirming the security over any transmission distance. Finally, results with complete system over fiber spools in laboratory are described, as well as over deployed fiber, are described in Section 4.5.

4.1 Implementation of the SSB system (d=0km)

The quantum key distribution system using the SSP principle encodes the information on the relative phase difference between an optical signal at frequency ω_0 and its modulation sidebands at frequencies $\omega_0 \pm \Omega$. To implement the system, two oscillators, synchronized at frequency Ω, drive two MZIs on Alice and Bob's sides. This modulation may also be done

with a phase modulator and a push-pull MZI. This last configuration allows in a practical point of view an easier tuning of working points. This is the configuration that will be used in our implemented prototype.

Let us recall the SSB principle, see Figure 53. The MZIs bias voltage correspond to phases $\Psi_1 = \pi/2$ and $\Psi_2 = -\pi/2$. The Alice and Bob's output signals are:

$$E_{\text{Alice}} = E_0 e^{j\omega_0 t} \frac{1 + j e^{jm\sin(\Omega t + \Phi_1)}}{2}, \tag{110}$$

$$E_{\text{Bob}} = E_{\text{Alice}} \frac{1 - j e^{jm\sin(\Omega t + \Phi_2)}}{2}. \tag{111}$$

The sideband amplitude after Bob's modulation is then:

$$i_{\omega_0+\Omega} = i_{\omega_0} \frac{m^2}{2} \cos^2\left(\frac{\Delta\Phi}{2}\right) \tag{112}$$

$$i_{\omega_0-\Omega} = i_{\omega_0} \frac{m^2}{2} \sin^2\left(\frac{\Delta\Phi}{2}\right), \tag{113}$$

where $\Delta\Phi = \Phi_1 - \Phi_2 + \dfrac{\pi}{4}$ and i_{ω_0} is the central peak intensity.

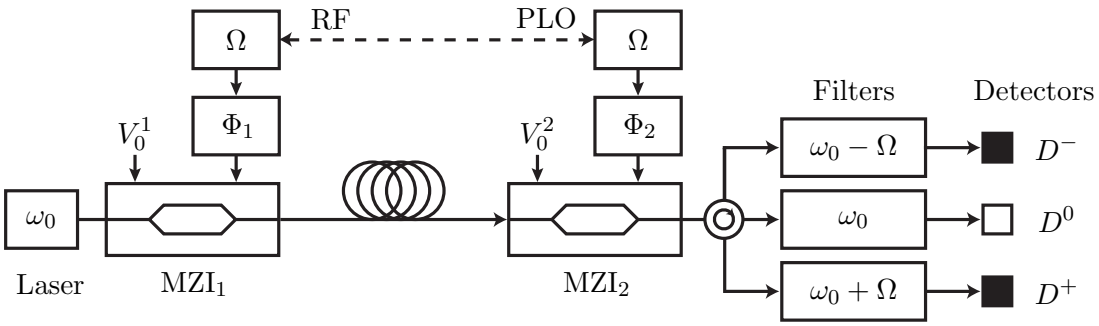


Figure 53: SSB principle implementation.

Each variable from the theoretical SSB principle description, such as ω_0, Ω, Φ_1, Φ_2, Ψ_1, Ψ_2, E_0, have to be chosen very precisely and rigorously. The implementation is split in blocks: first block includes the optical line, i.e., the laser diode and MZI modulators, see Section 4.1.1. The second block includes the HF electric line that drives the MZIs, see Section 4.1.2. Finally, the filtering and signal detection at frequencies $\omega_0 + \Omega$ and $\omega_0 - \Omega$ is described in Section 4.1.3.

4.1.1 Optical Line

4.1.1.1 Laser Source

The implemented system is designed to work on optical fibers for a wavelength in the 1550nm order, allowing benefiting from all the today's available technology of standard telecom. A 1547.43nm laser diode is used. It has a 5MHz ray thickness, which is thin enough to be able to use the SSB modulation scheme.

4.1.1.2 Optical signal modulation - MZI

The used modulator is an electro-absorbent directly integrated ahead the laser diode. The modulators bandwidth is about 5GHz. We then can use a 2GHz modulation frequency Ω. The modulation depth may be determined with the modulation electric signal power.

4.1.1.3 Attenuators at the source

The system includes a programmable attenuator that allows one to quickly and easily switch from classical mode, where Alice sends an average energy of 1 milliwatt per pulse, to the quantum mode, where Alice sends a signal with about one photon per pulse on average in both sidebands.

4.1.2 Modulation HF Circuit

4.1.2.1 Synchronization et stability

The hyper frequency circuit includes the main oscillator. We use a tunable Anritsu™ generator. To be able to precisely tune the initial phase shift Φ_1 of the signal at frequency $\Omega = 2\text{GHz}$, we use an electric phase shifter driven by a continuous voltage.

First, Bob's oscillator at frequency Ω is the same as Alice's, guaranteeing *de facto* their synchronization.

4.1.3 Filtering and Measure

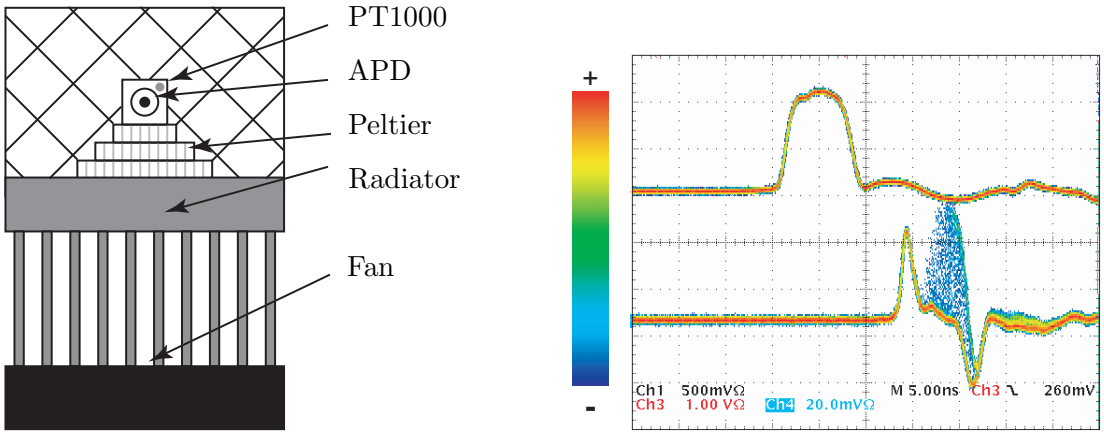
4.1.3.1 Filters for D^+ and D^-

To separate frequencies $\omega_0 - \Omega$ and $\omega_0 - \Omega$, we use a Fabry-Pérot fibered filter that presents 2dB losses, a 100GHz ISL, a finesse of 100, and a resolution of 100MHz.

4.1.3.2 Quantum Detection

To detect the incident photon, a heavily cooled avalanche photodiode system is used. An incident photon on the avalanche diode (APD) produces in the device an avalanche phenomena that creates a macroscopic and detectable current, see Figure 54(b).

The diode EPITAXX EPM 239 may work at temperatures in the -60℃ to -40℃ range that my be obtained thanks to a three stages Peltier module, see Figure 54(a). The module is glued on its cold side to a metal block for thermal inertia in which is sticked the APD and a thermal probe PT1000. The Peltier hot side is glued to a radiator and a fan to dissipate produced heat and to maintain the radiator at room temperature, see Figure 54(a). To maintain the temperature constant, a PID control is built on the Peltier with an external circuit. The measured temperature fluctuations are in the 0.1℃ order when the diode is in -55℃ steady state after 18min setting time.



(a) Temperature Control.

(b) Detected Current for the Diode.

Figure 54: Photodiode and detected current.

Dark count hits create errors and lowers drastically the maximum attainable distance. It is possible to reduce the noise errors by placing the diode in a state where it can create an avalanche only during a useful window, i.e., only when the diode is supposed to receive an pulse incident photon. The precision of the clock sent by Alice is ±500ps, allowing to precisely set a gate of 1ns broader than the pulse. This mode is called *active gating*. The polarization voltage is modulated around a given value $V_A = 50,1\text{V}$, slightly below the breakdown voltage $V_B = 48V$. The modulation voltage is made of detection gates that last

$\tau_{\text{gate}} = 8\text{ns}$, which is over the optical pulse duration time $\tau_{\text{opt}} = 7\text{ns}$, see Figure 55. The diode polarization voltage becomes temporarily greater than the breakdown voltage, which allows the avalanche when there is an incident photon. The voltage V_B allows the diode to relax and to eliminate all remaining electrons in the material.

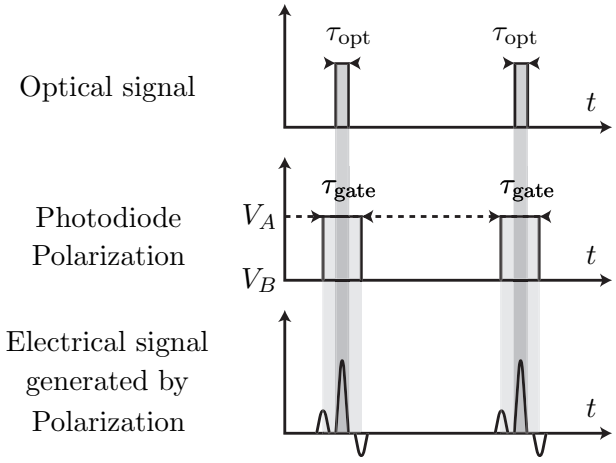


Figure 55: APD photon detection chronogram.

An unwanted effect with the APD is the after pulses. These are pulses that appear when the diode did not had time to relax its material from all electrons, creating then an unwanted avalanche. For a -55℃ temperature, the after pulsing is about 2% for a relaxing time of 1μs. The diode is then used at a 1MHz frequency. The relaxation time imposes a strong limitation on the emission rate and bit reception, thus limiting the final key rate.

4.1.4 Principle global test - Visibility

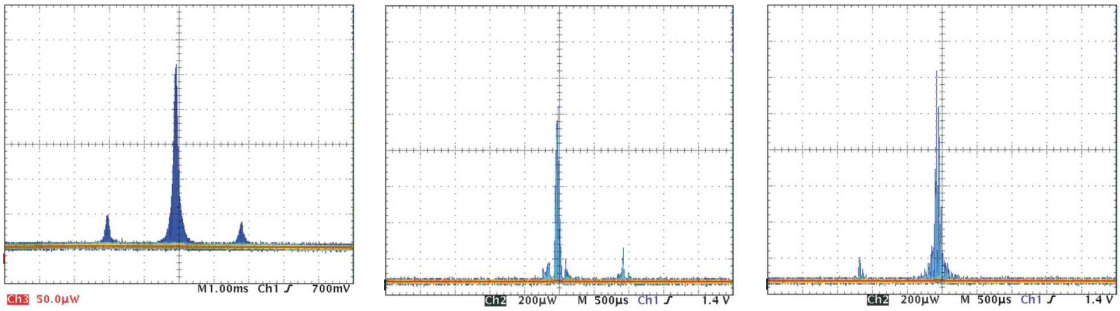
The SSB global system is built on two different tables for Alice, see Figure 56(a) and for Bob, see Figure 56(b).

The used configuration allows one to verify the sidebands behavior as a function of phase difference $\Delta\Phi$ between emitter and receiver oscillators. A Fabry-Pérot filter is used as spectrum analyzer by applying a variable voltage to shift the filtering central frequency. One can then observe the signal spectrum amplitude, see Figure 57. The Figure 57(b) and Figure 57(c) represent Bob's output when phase difference $\Delta\Phi$ is 0 or π. Measured visibility is then 99% and stays at this level in any working mode.

Then, it is possible to apply the SSB principle to perform quantum key distribution

(a) Alice's apparatus (b) Bob's apparatus

Figure 56: SSB principle quantum key distribution prototype.



(a) $\Delta\Phi = \pm\pi/2$ (b) $\Delta\Phi = 0$ (c) $\Delta\Phi = \pi$

Figure 57: Signal spectral density in classical mode for different phase difference values $\Delta\Phi$. The observed visibility is about 99%.

between Alice and Bob.

4.2 Automatic bit generation and counting

To implement the SSB principle in an efficient manner, it is important to perform the information encoding and measurement with computer driven apparatus. Two elements should be taken into account to have an efficient transmission management: hardware interfaces and compatible software.

Digital data acquisition and generation from National Instrument (NI) are to be installed in computers and allow one to generate a driving signal and to acquire measurement results for long bit string transmissions. The interfaces between prototype elements and NI cards are described in Section 4.2.1. Then the Labview software[1], today's standard in many research laboratories, presents many advantages that may be use in our experiment. This tool is installed in computers that include NI cards and allow one to control prototype driving signals, see Section 4.2.2.

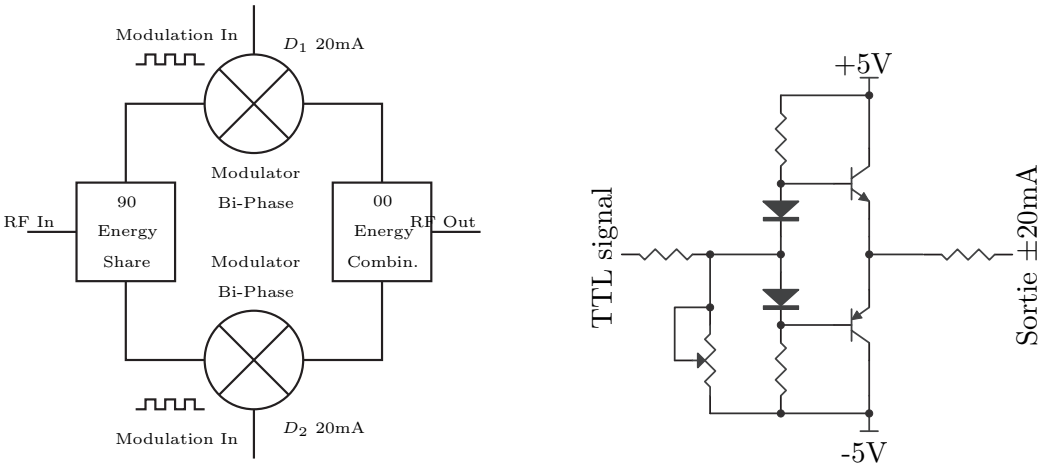
4.2.1 Hardware interfaces

4.2.1.1 QPSK commands

The information encoding is done by choosing the phase Φ_1, i.e., the oscillator initial phase at frequency Ω, that drives MZI_1, see Figure 53. Phase Φ_1 is chosen among four possible values 0, $\pi/2$, π, and $-\pi/2$ thanks to a PULSAR MT-B6-0233 quadrature phase shift keying modulator (QPSK) driven by two signals D_1 and D_2 with a $\pm$20mA current, see Figure 58(a).

To drive the QPSK module with a computer binary signal at frequency in the MHz range, we have chosen a National Instrument PCI6534 card. Output signals are TTL format (0-5V). We have then built an interfacing card $\pm 20\text{mA} \leftrightarrow 0-5\text{V}$, see Figure 58(b). It allows also to quickly adapt the PCI card SCSI connectors and the PQSK module SMA ports.

[1]Labview is a graphical development tool from National Instrument.



(a) QPSK modulator principle.

(b) Electronic drawing for QPSK card

Figure 58: QPSK modulator principle. The QPSK modulators reference is Pulsar MT-B6-0233.

4.2.1.2 Detection and counting

The photon detection within the pulses is made thanks to a previously described avalanche photodiode, see Section 4.1.3.2. The data acquisition is performed thanks to a National Instrument PCI6024E computer card interfaced with multi stage electronics, including a comparator, an amplificator, and a monostable used to lengthen the pulses, see Figure 59.

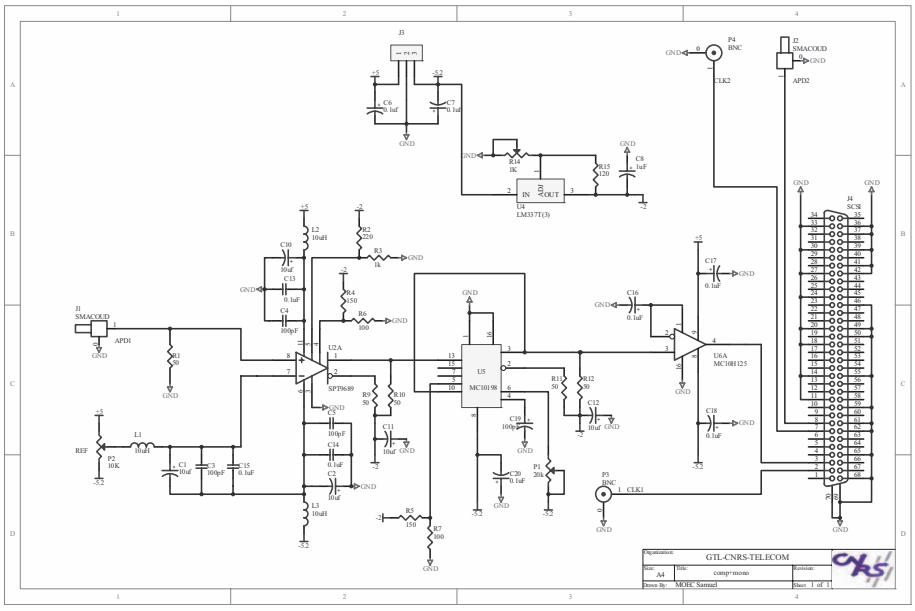


Figure 59: APD electronic design for APD pulses detection.

The photon detection at very specific times allow one to activate photon detectors at

also very precise time windows, highly lowering false detections, the *dark count*, inducted by the APDs, see Section 4.1.3.2, thus increasing the observed QBER. A clock signal is generated by Alice and transmitted to Bob to synchronize the pulse generation and the information encoding.

4.2.2 Software interface

The NI cards may be driven from different computer programs. The Labview software presents a graphical interface for simple and direct application design and extension card control. The NI cards commands, thanks to C++ programs, allow one to build program modules that may be then integrated in larger programs.

The program developed with Labview includes two windows. The first one, the *front panel*, is the final interface with which the operator interacts in front of the computer. This window includes indicators, push buttons, and value fields to enter commands. The second one, the *back panel*, is the program schematic, the program core. It shows how the different indicators interact with the NI cards for example.

4.2.2.1 QPSK control

The PCI6534 card command program allows one to generate many TTL digital signals. Two signals are generated for the QPSK command and a third signal is used as clock signal to allow synchronization for pulse detection on Bob's side. A chronogram of the three signals is represented on Figure 60.

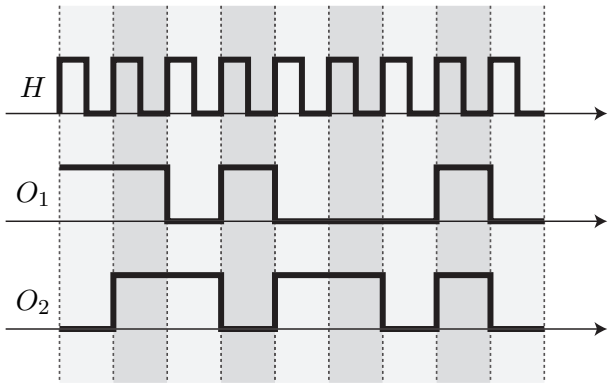


Figure 60: Chronogram of the QPSK command signals. H is the clock signal, O_1 et O_2 are the QPSK command signals.

A random bit string generation module is implemented and "encapsulated" in a labview subprogram. The front panel includes indicators (-) and commands (*) to control the generated signals, see Figure 61(a):

- Encoded bits

- Bases

- Clock frequency

- bit numbers in the bit string

* On/Off for bit string randomness

* On/Off for the bases randomness

* On/Off to activate the clock signal

* On/Off for bit string saving

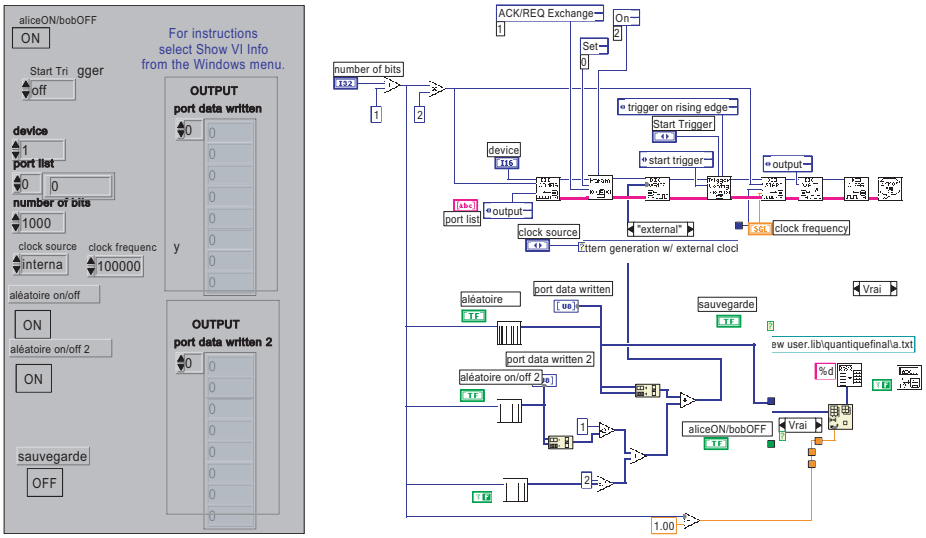
The back panel includes the command bock chain for the NI cards, as well as the bit string building chain, see Figure 61(b). The program includes also the possibility to save the bit string to proceed the following classical reconciliation steps afterward. One can notice the clock signal generated by the program.

4.2.2.2 Detection control

The pulse counting from the APD interfacing circuit is a simple operation that is then done by a simple program. The clock count between each pulse from the diode is saved. Then, we can deduce the arrival time for each pulse, see Figure 62. The program includes also a button that allows to save the results, i.e., the detected pulses positions.

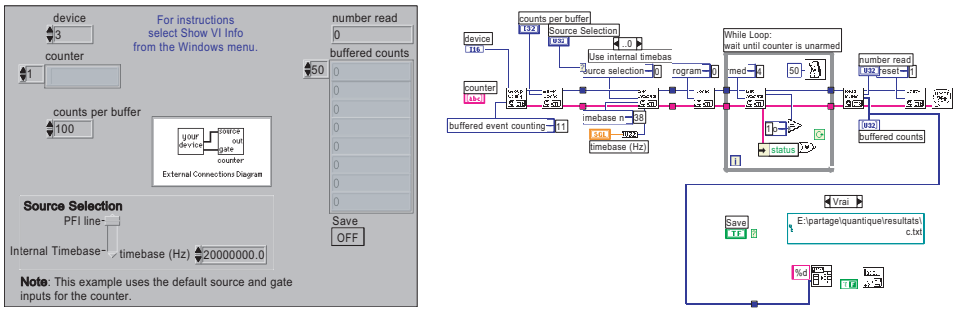
4.2.3 Global test for generation and bit counting

In the experiment, with an initial 1MHz rate, the clock signal transmitted by Alice allows Bob to synchronize his QPSK command signal. The signal rising edges indicate a bit slot change. For each rising edge detected by Bob, the QPSK control signal change the value



(a) Control front panel. (b) Program design on the back panel.

Figure 61: QPSK labview command.

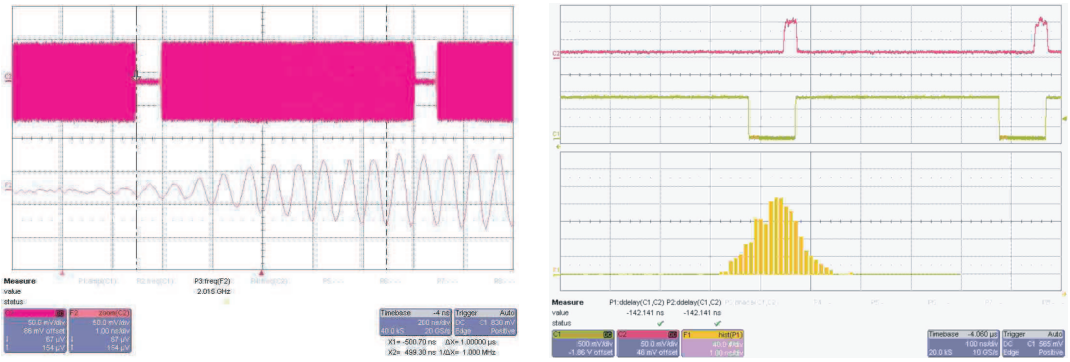


(a) Control front panel. (b) Program design on the back panel.

Figure 62: Compting labview command

that correspond either to the bit or the next basis, see Figure 60. The clock allows also the counting card to count the bit slot number that correspond to the gray parts, see Figure 60. For each bit slot, the QPSK control value stays the same, allowing the 8ns optical pulse to be positioned anywhere in 1μs slot.

The limitation for the temporal synchronization is based on the precision of the clock signal transmission. The signal recuperation is performed with the synchronization signal envelope detection, see Figure 63(a). As the detector bandwidth is limited, it is not possible to obtain a perfect square signal. The clock signal rising edges are less sharp, which inducts a drift in the clock tics detection within the 1ns range, see Figure 63(b). The small drift allows one to implement 10ns long detection windows for 8ns long pulses.



(a) HF Signal modulated by the clock signal. (b) Detection drift for clock signal.

Figure 63: Clock signal

The bit strings used to encode the bits and phases by Alice, as well as the Bob's bases bit string and bit detection string, are saved to perform transmission reconciliation and to extract finally a secret bit string. Bob sends to Alice on the public channel the bit times where he has detected a photon. Alice tells him then what bases she used to encode information in the pulses. Alice and Bob perform a transmission in classical mode to test the apparatus, see Figure 64. They keep only the bits where the basis match, see Table 9.

The public comparison is made on the public channel. Alice and Bob share about 20% of the key on the public channel to evaluate the quantum bit error rate QBER_{approx}. With this estimation, they implement an adapted error correction. The exchanges for the reconciliation and error correction are directly implemented in a C++ software. It is

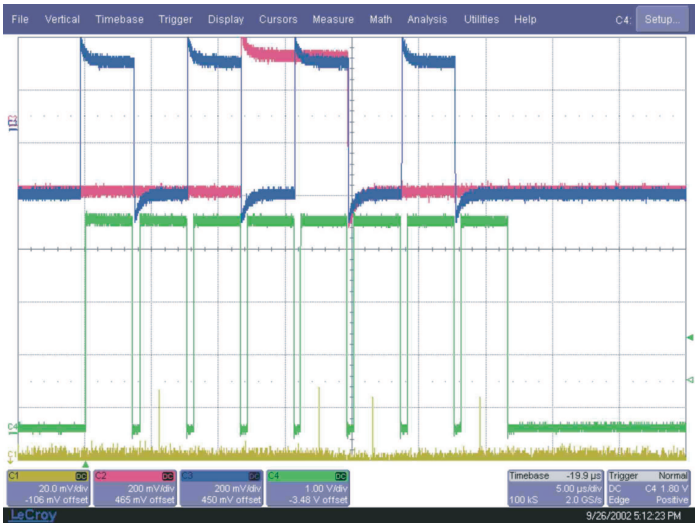


Figure 64: QPSK modulation test

Table 9: Bit reconciliation between Alice and Bob. • shows non matching basis, Y shows matching basis.

Alice Basis	0	1	0	1	0	1	0	0	1	1	1	0	1	0	1	1	0
Alice Bits	0	0	1	0	1	1	0	1	1	1	1	1	0	1	0	1	0
Bob Bases	1	1	1	0	1	0	1	0	1	0	0	1	0	0	0	0	0
Bob Bit Detection	0	0	1	0	1	1	1	1	1	0	0	1	0	1	0	0	0
Matching Basis	•	Y	•	•	•	•	•	Y	Y	•	•	•	•	Y	•	•	Y
Shared Bit		0						1	1					1			0

possible then to develop the NI cards interfacing with C++ for signal generation and pulse counting. This allows one to have a single program for the whole application.

4.3 Propagation and optical path fluctuation compensation

The quantum channel between Alice and Bob is an optical fiber. It is then very sensitive to external variations, and most precisely temperature variation that make the fiber length change, changing the optical path length as well.

When considering the propagation constant β_0 for frequency ω_0, it becomes $\beta(\omega)$ for a frequency ω close to ω_0 [2]:

$$\beta(\omega) = \beta_0 + \beta_1(\omega - \omega_0) + \frac{\beta_2}{2}(\omega - \omega_0)^2. \tag{114}$$

Propagation is indeed different for different frequencies. This does influence our system as the SSB scheme relies on a multiple frequency signal. Though, this propagation difference may be corrected at the first order. An auto-compensation signal that travels through the same medium is deformed with the same constraints as the quantum signal. The exact use of this signal is described in Section 4.3.1. This signal allows a very high stability of the experiment over time, see Section 4.3.2.

One may notice that our system does not use or depend on polarization of the optical signal. Though some of the device we are using, such as the MZIs, have an efficiency that is sensitive to the input signal polarization. We have then implemented a system to control the polarization variations over time, see Section 4.3.3.

4.3.1 Theoretical description of the auto compensation technique

4.3.1.1 Signal and propagation

When one considers a multiple frequency signal that propagates on a fiber, one should take into account the propagation constant$\beta(\omega)$, see Equation (114). Let us consider a light field E_1 before propagation:

$$E_1(t) = E_0 A(t) e^{j\omega_0 t}, \tag{115}$$

where E_0 is the signal real amplitude, and $A(t)$ its complexe phase. After propagation over a distance l, the light field E_2 is:

$$E_2(t) = \frac{E_0}{2} e^{j\omega_0 t + \beta_0 l} \left[FT \left[FT^{-1} \left(A(t) \right) \right]_{t'=t-\beta_1 l} \right]. \tag{116}$$

Alice and Bob are located at a distance l from each other. When we consider this distance to be constant, $l = l_0$, all signal phases rotate by $\beta_0 l$. Moreover, the relative phase difference between the central peak and its sidebands is $-\beta_1 \Omega l_0$ for frequency $\omega_0 + \Omega$, and is $\beta_1 \Omega l_0$ for $\omega_0 - \Omega$ at first order. Then, on may consider that phase encoded in the signal is $\Phi_1' = \Phi_1 - \beta_1 \Omega l_0$. Though, this may be exactly compensated at emitter or receiver. The unbalanced rest is due to the β_2 constant and may be neglected here.

The signal at Alice's modulator output is propagating in the fiber, see Equation (110). As of Equation (116), after propagation over a distance l, the signal E_{Alice} becomes:

$$E'_{\text{Alice}} = \frac{E_0}{2} e^{j(\omega_0 t - \beta_0 l)} \left(1 + j - \frac{m}{2} \left(e^{j(\Omega t + \Phi_1 - \beta_1 \Omega l + \frac{\beta_2}{2}\Omega^2 l)} + e^{j(-\Omega t - \Phi_1 + \beta_1 \Omega l + \frac{\beta_2}{2}\Omega^2 l)} \right) \right). \tag{117}$$

One may observe that the relative phase difference between the central peak and the sidebands varies as a function of propagation distance variations. The signal after Bob's modulation is then:

$$\begin{aligned} E'_{\text{Bob}} = & \frac{E_0}{8} e^{j(\omega_0 t - \beta_0 l)} \Big[8 \\ & + jme^{j\Omega t}(1+j) e^{\frac{j(\Phi_1 + \Phi_2 - \frac{\pi}{2})}{2}} \left(e^{j(\frac{\Delta\Phi}{2} - \frac{\beta_1}{2}\Omega l + \frac{\beta_2}{4}\Omega^2 l)} + e^{-j(\frac{\Delta\Phi}{2} - \frac{\beta_1}{2}\Omega l + \frac{\beta_2}{4}\Omega^2 l)} \right) \\ & - jme^{-j\Omega t}(1-j) e^{\frac{-j(\Phi_1 + \Phi_2 - \frac{\pi}{2})}{2}} \left(e^{j(\frac{\Delta\Phi}{2} - \frac{\beta_1}{2}\Omega l - \frac{\beta_2}{4}\Omega^2 l)} + e^{-j(\frac{\Delta\Phi}{2} - \frac{\beta_1}{2}\Omega l - \frac{\beta_2}{4}\Omega^2 l)} \right) \Big]. \end{aligned} \tag{118}$$

One can compute the sidebands amplitude:

$$i_{\omega_0 + \Omega} = \frac{(mE_0)^2}{16} \cos^2 \left(\frac{\Delta\Phi}{2} - \frac{\beta_1}{2}\Omega l + \frac{\beta_2}{4}\Omega^2 l) \right), \tag{119}$$

$$i_{\omega_0 - \Omega} = \frac{(mE_0)^2}{16} \sin^2 \left(\frac{\Delta\Phi}{2} - \frac{\beta_1}{2}\Omega l - \frac{\beta_2}{4}\Omega^2 l) \right). \tag{120}$$

To compare the system in an homogeneous manner, it is possible to measure the visibility V as defined by:

$$V = \frac{i_{\max} - i_{\min}}{i_{\max} + i_{\min}}. \tag{121}$$

The system is tuned to have maximum visibility for $l = l_0$. We consider distance fluctuations with $l = l_0 + \delta l$. The terms $i_{\max}$ and $i_{\min}$ are defined for $\Delta\Phi - \beta_1 \Omega l_0 = 0$ et $\Delta\Phi - \beta_1 \Omega l_0 = \pi$. Considering $\beta_1 \gg \beta_2 \Omega$, each sideband visibility is then:

$$V_{\omega_0+\Omega} = \cos\left(\beta_1 \Omega \delta l\right), \tag{122}$$

$$V_{\omega_0-\Omega} = \cos\left(\beta_1 \Omega \delta l\right). \tag{123}$$

The visibility drift is very important with the optical path fluctuations. With a standard fiber and a frequency $\Omega = 2$GHz, the coefficient $\beta_1 \Omega$ is about 60 rad/m. With such value, one must maintain the fiber length within a 0.1 mm range. This is extremely difficult over long fiber distances. One may notice that visibility do not depend on the modulation depth m.

4.3.1.2 First order drift auto-compensation.

It is possible to obtain a tremendous increase for the visibility by compensating the phase difference due to optical path fluctuations. This may be done by using a phase reference signal propagating in the same fiber at a very close wavelength. This signal follows the same optical path fluctuations and then may be used to compensate the information signal at frequency ω_0

An optical field is produced by a laser diode at frequency ω_0. This signal is modulated with an MZI driven by the same HF signal than the quantum line, at frequency Ω =2GHz. The multiplexed signal is transmitted on the same optical fiber as the quantum channel, and will thus follow the same perturbations. This signal is then extracted and detected to obtain the HF electrical signal to modulated the quantum channel, see Figure 65.

The synchronization optical signal is of the same form as Alice's quantum signal, see Equation (110). Then amplitude modulation detection of the optical signal after propagation generates a signal of form:

$$V_{\mathrm{HF}} = a \cos(\Omega t - \beta_{1s} \Omega l) \cos\left(\frac{\beta_{2s}}{2} \Omega^2 l\right), \tag{124}$$

where a is a coefficient that depends on the detector efficiency and the signal amplification. This signal electric phase does depend directly on the optical path length, and thus depends

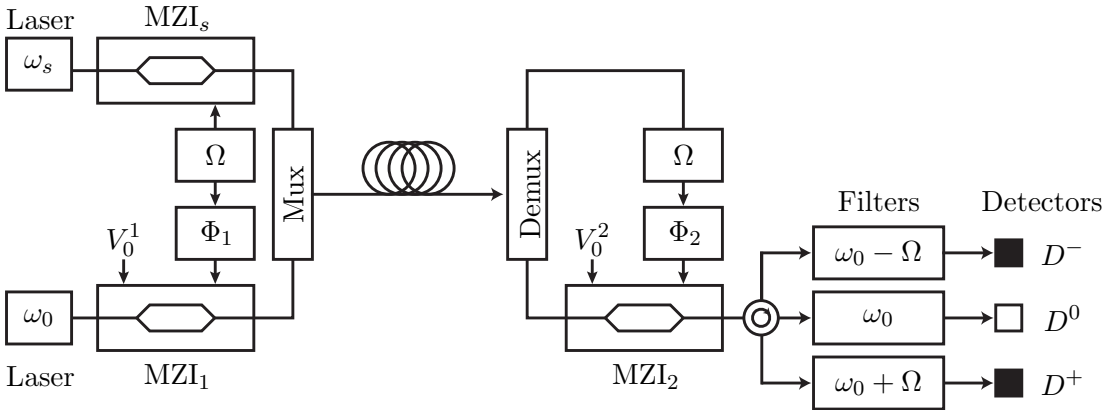


Figure 65: Synchronization system.

on its fluctuations as well. This signal is used to directly modulate Bob's MZI, MZI_2. Bob's sidebands amplitude are with synchronization:

$$i_{\omega_0+\Omega} = \frac{(E_0 m)^2}{16}\left(1+\cos\left(\frac{\beta_{2s}}{2}\Omega^2 l\right)\right)\left(1+V\cos\left(\Delta\Phi+\Omega l(\beta_1-\beta_{1s})-\frac{\beta_2}{2}\Omega^2 l\right)\right) \quad (125)$$

$$i_{\omega_0-\Omega} = \frac{(E_0 m)^2}{16}\left(1+\cos\left(\frac{\beta_{2s}}{2}\Omega^2 l\right)\right)\left(1-V\cos\left(\Delta\Phi+\Omega l(\beta_1-\beta_{1s})+\frac{\beta_2}{2}\Omega^2 l\right)\right) \quad (126)$$

where $V = \dfrac{2\cos\left(\frac{\beta_{2s}}{2}\Omega^2 l\right)}{1+\cos\left(\frac{\beta_{2s}}{2}\Omega^2 l\right)}$. The phase speed difference may be approximated as follows:

$$(\beta_1-\beta_{1s})\Omega l \approx (\omega_0-\omega_s)\beta_2\Omega l. \quad (127)$$

Then, in the same fashion, visibility is as follows:

$$V_{\omega_0+\Omega} = \cos\left(\beta_2\Omega\Lambda\delta l\right), \quad (128)$$

$$V_{\omega_0-\Omega} = \cos\left(\beta_2\Omega\Lambda\delta l\right), \quad (129)$$

where $\Lambda = \omega - \omega_s$. The visibility is now much less sensitive to the optical path fluctuations δl.

4.3.2 Auto compensation implementation and test

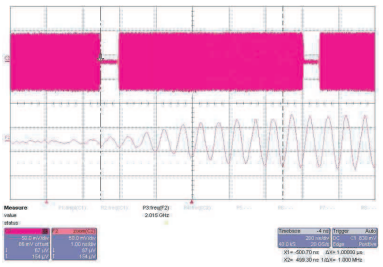
The synchronization signal is generated by a direct modulation laser diode at wavelength $\omega_s = 1552.43$nm, that is 5nm distant from the quantum channel. The signal energy is lowered down to 600μW so is enough to be detected after tens of kilometers without creating

"crosstalk" with the quantum signal. The optical signal is then added to the quantum signal thanks to a mixer.

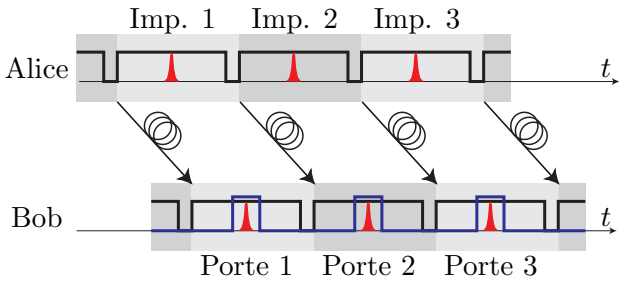
On Bob's side, the quantum signal and the synchronization signal are separated by an *add & drop* filter. The synchronization signal at frequency ω_s is detected by an envelope detector to extract the signal at frequency Ω. This last electric signal is transmitted through a QPSK whose phase switches between $\{0, \pi/2, \pi, -\pi/2\}$. This signal is used to drive the modulator of the quantum signal, compensating eventually the phase drift due to optical path difference, as described in Section 4.3.

The synchronization signal from Alice's oscillators is also used to transmit the pulses temporal synchronization. The optical carrier at frequency ω_s is modulated by the HF signal. It is also amplitude modulated by a square shape clock signal whose frequency is the pulse rate 1MHz. The signal that modulates Alice's MZI for synchronization is represented on Figure 66(a). The optical signal received by Bob goes through a power splitter and then a mixer that allows detecting the square envelope at clock frequency. The clock signal is used by Bob to synchronize the signal generation to control the QPSK and to regulate very precisely the active gating and photon detection.

The clock signal is used to trigger the pulse generation by Alice that is located about at the middle of the bit slot, see Figure 66(b). Then, as the pulses and the clock signal propagate on the same fiber, the clock signal allows to determine exactly the pulse temporal position. The detection gates are set very precisely just around the pulses, see Figure 66(b), lowering by much the detection errors.



(a) Synchronization signal modulation.



(b) Clock signal transmission principle.

Figure 66: Clock signal transmission.

The result of the amelioration with the auto-compensation system is described in Figure 67. The experimental results are obtained by simply adding some optical path lengths thanks to a fibered delay line for lengths from 1mm to 10cm in free space, and optical fiber pieces from 1m to 60m. Though we did not reach 99% visibility, we showed that visibility is not altered by changing the fiber length.

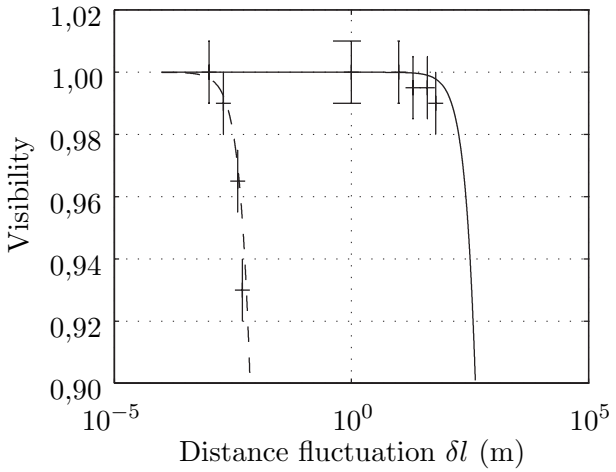


Figure 67: Signal visibility with and without synchronization. The visibility without synchronization is represented in dashed line, and the visibility with synchronization is represented in plain line. The visibility gain with the synchronization line is of many decade orders.

4.3.3 Polarization

The polarization in an optical fiber is a difficult variable to control. Though the SSB principle is not sensitive to input polarization, the physical devices are sensitive to input polarization. The MZI modulators are in Lithium Niobate, $LiNbO_3$. They are in Z cut to have low losses, but need to have the input polarization aligned along this cut.

The system visibility depends practically on the polarization control. The quantum line polarization may evolve over time, and decreasing the visibility. Though, the synchronization signal suffers the same polarization fluctuations, it may then be used as polarization reference to track the drift on the quantum line.

The polarization is measured on the synchronization line, and the correction is applied on the quantum line. A polarization controller applies two rotations on the polarization, see Figure 68. One may notice that two rotations are necessary to correct any variation.

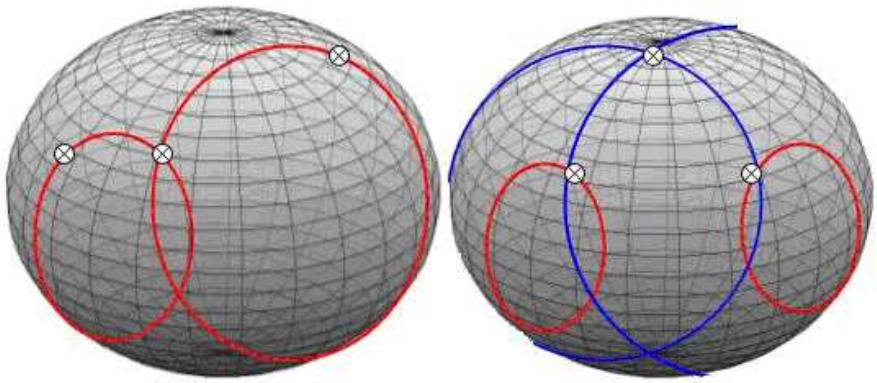


Figure 68: Stokes vector visualization in the Bloch ball.

The polarization active control is realized with Labview, see Figure 69. A stokes vector visualization in the Poincaré sphere allows one to apply the desired control.

The active polarization control allows one to correct the polarization variations that have a frequency up to tens of Hertz. Polarization rotation angles to be applied as correction are tabulated in a separated library, programmed in C++ to increase performance.

4.4 Reference Implementation

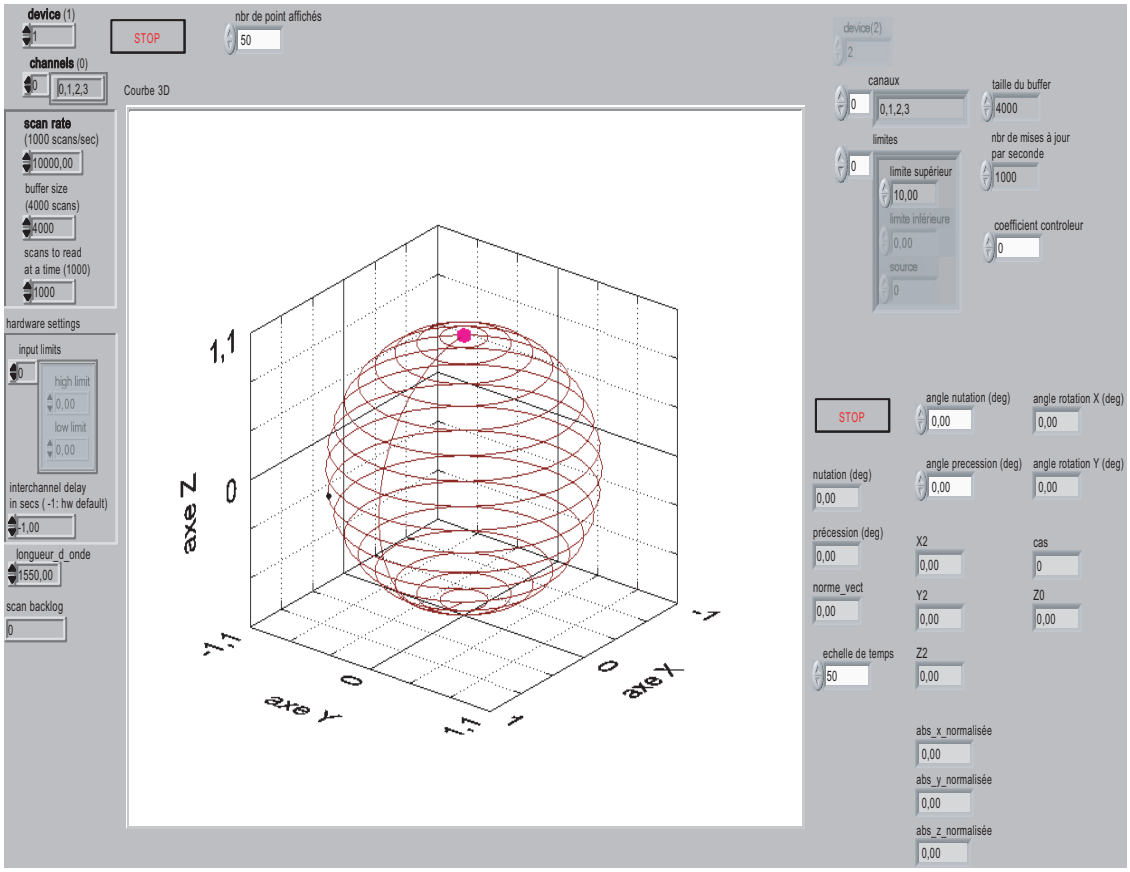
The SSB system uses a fainted laser diode as photon generator. It is thus sensitive to the PNS attack. Though, it is possible to implement the central peak detection as strong reference to make the system resistant against the PNS attack. The system modification to detect the reference signal at frequency ω_0 is described in Section 4.4.1.

4.4.1 Hardware modification for reference detection

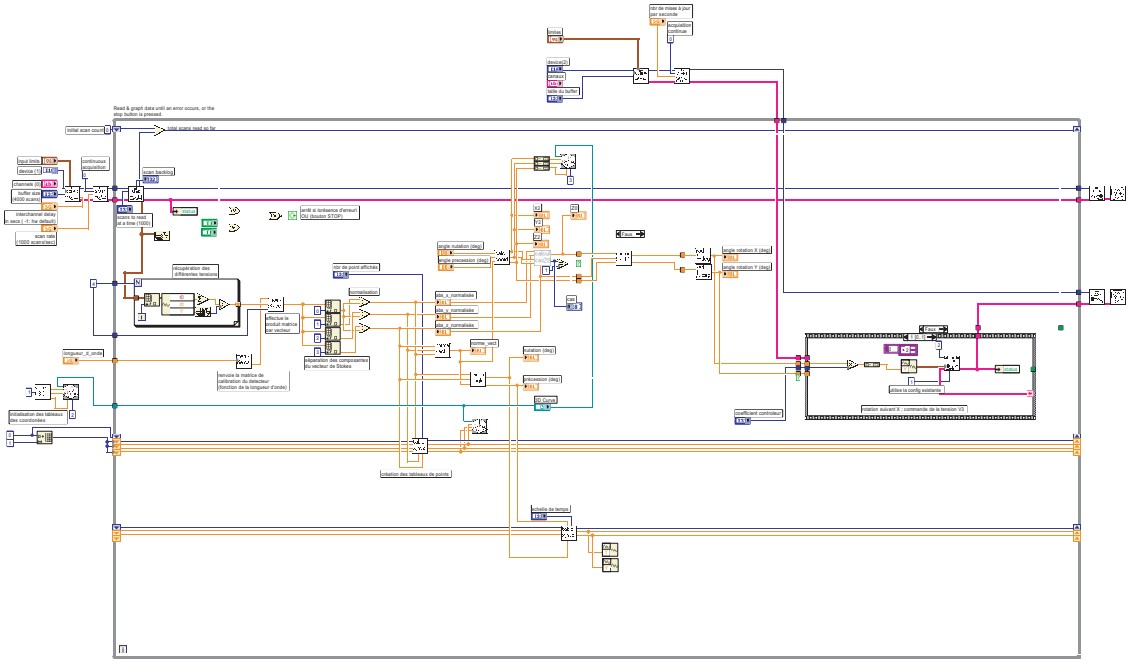
The *strong reference* signal detection is performed by modifying the system to add a filtering at frequency ω_0. A circulator is added right before the second frequency $\omega_0 + \Omega$ detection, then a quantum or classical detector is used, as a function of the signal awaited power, see Figure 70.

4.5 Final results, transmission, and performance

The global system is implemented and tested on fiber spools for distances of tens of kilometers, allowing one to validate the principle for long distances. To guarantee absolute



(a) Polarization control front panel.



(b) Polarization control back panel.

Figure 69: Labview panels for polarization control.

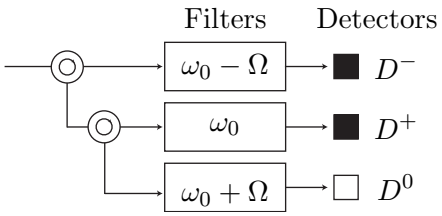


Figure 70: Apparatus for reference detection

security, the observed error rate, the QBER, must be lower than 15%.

4.5.1 Transmission and QBER

The transmission error rate is measured as a function of distance. It is defined as the ratio of errors detected over effective detected bits. The theoretical quantum error rate $\mathrm{QBER}_{\mathrm{theo.}}$ may be estimated as follows [46]:

$$\mathrm{QBER}_{\mathrm{tho.}} \approx \frac{1}{2} \cdot \frac{(1-V)P_{\mathrm{signal}} + P_{\mathrm{dark}}}{P_{\mathrm{dark}} + P_{\mathrm{signal}}}, \tag{130}$$

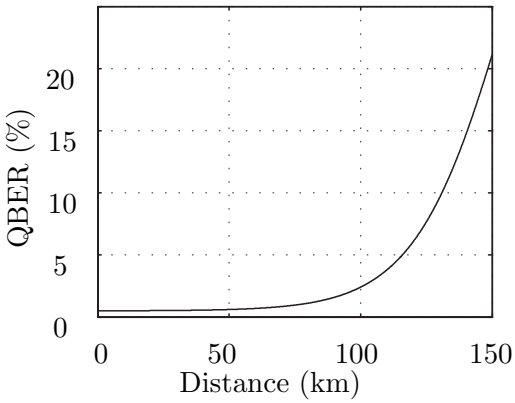
where $P_{\mathrm{signal}} = 1 - e^{\mu\eta T}$ is the awaited probability of counts, μ = photon per pulse is the average power at Alice's output, η is the detector quantum efficiency, $T = 2.8$dB is the overall losses due to the receptor and transmission losses, $V = 98\%$ is the visibility, and $P_{\mathrm{dark}} = 8 \cdot 10^{-6}$ is the dark count probability. The QBER as a function of the distance is showed on Figure 71(a). The measured visibility is 98% and the fiber losses are 0.25dB/km.

4.5.2 Comparison with existing systems

The British Telecom group has developed a system where the encoding relies on the phase difference between two time separated pulses thanks to a strongly unbalanced interferometer. Though, this system is very sensitive to external disturbance such as temperature of vibrations.

The Los Alamos group presents a close system where the phase encoding is used in the time domain, with similar results over 48km distance.

The Geneva group has developed their *Plug&Play* system as described earlier. They show a final 210 Hz bit rate. A communication over 67km has been performed between Geneva and Lausanne.



(a) Quantum error rate QBER as a function of distance d in km.

(b) Deployed fiber over the Technople area.

Figure 71: Error rate and deployed fiber.

The NEC Lab group showed that a single photon interference over 100km with using an unbalanced detector in active gating mode and a Plug&Play system for transmission. The visibility with 0.1 photon per pulse is over 80% after 100km. This corresponds to fidelity of a cryptographic system of more that 90% and a QBER of less than 10%, satisfying the security criteria to extract a secret key.

The Toshiba UK group uses a phase modulation system with a Mach-Zehnder system. The final rate is 15Hz for a 101km distance.

All these results are tabulated in Table 10.

Research group	λ (nm)	d (km)	μ	F (kHz)	$D_{\mathbf{raw}}$ (Hz)	Q (%)
B.T [65]	1300	25	0,15	1000	500	2
Los Alamos [37]	1300	48	0,63	100	20	9,3
Genve [63]	1550	67	0,2	5000	160	5,6
Nec Lab. [44]	1550	100	0,2	500	5.5	10
Toshiba [75]	1550	101	0,1	500	15	7,1
G.T.L. [35]	1550	40	0,2	1000	40	3
G.T.L. (Avec *strong reference*)	1550	120	1	1000	1000	8

Table 10: Experimental results of other groups.

With commercially available components, our system compares favorably with other quantum key distribution systems.

4.5.3 Secure bit rate measure

This error rate directly influences the final key rate. Thus, it is computed as a function of the transmission distance, see Figure 72.

From Shannon's theory, the key rate after error correction is [63]:

$$D_{\text{net}} \approx \Bigg(1 + Q\log_2(Q) - \frac{7}{2}Q \\ -(0,03 + I_{\text{multi}})\left(1 - (1-Q)\log_2(1-Q) - \frac{7}{2}Q\right)\Bigg) D_{\text{brut}}, \tag{131}$$

where I_{multi} is the information leaked to Eve from the multiphoton pulses.

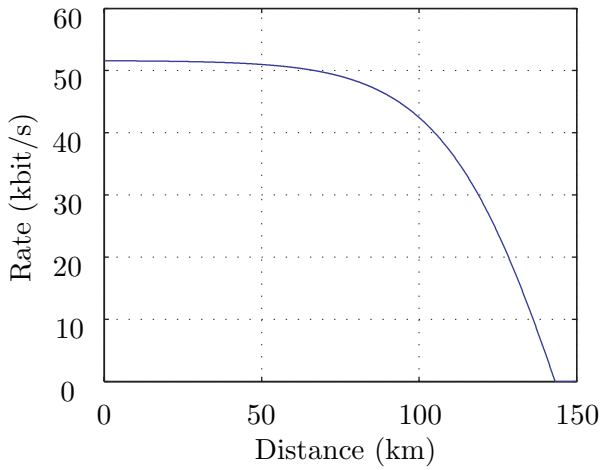


Figure 72: Final key rate as a function of distance.

One may observe that the transmission key rate drops only slightly until 100km distance. It is realistic to consider that a transmission may be realized over 120km fiber distance.

4.6 Conclusion

Practical aspects of the QKD prototype implementation have to be considered very precisely to guarantee performance close to theory. Particularly, the system performances are optimized to maximize Bob's detector visibility in non-quantum mode. The error rate is mainly linked to the APD dark count. The detection gates duration is lowered to the maximum to avoid false detections. It may also be verified that interference between multiple frequency signals may be considered as negligible.

The system stability core is the oscillators' synchronization and the detection windows.

A new technique has been implemented to compensate temporal fluctuations of the quantum channel. The optical path fluctuations between Alice and Bob, due to physical environment variations, are compensated exactly at first order with the autocompensation. A signal is sent on the same optical fiber with a slightly different wavelength to compensate exactly the same optical path fluctuations, thus compensating the visibility fluctuations on the optical phase. The theoretical aspects, practical implementation, and automatization have been described.

The last contribution to this chapter relies on the strong reference QKD protocol implementation. This system may then use a fainted laser source where the source may have on average one photon per pulse. This strong power allows increasing the secure bit rate to much higher rates and distances. The rate for very long distances is limited mainly when the reference signal intensity is very low, though without reducing the security.

CHAPTER V

CONCLUSION AND PERSPECTIVES

Classical cryptography has developed information encryption algorithms very efficient for theoretical security, but are harder to implement and slow to run. To guarantee transmission confidentiality, this theoretical property relies on an encryption key that has to be kept *secret*, i.e., known only by the authenticated parties. Public key algorithms are implemented to transmit encryption keys, but their security relies on mathematical conjectures that could be broken in the future. Thus, they cannot be fully trusted. Moreover, it is theoretically impossible to generate secret with a classical channel, i.e., a channel that anybody may read and copy. Quantum cryptography solvess this problem. It enables secret key transmission, or secret growing between remote parties.

Quantum key distribution generates remotely a secret key between Alice and Bob. This key may then be used, with the one time pad algorithm for example, to perform secure transmission guaranteed by physical properties and information theory. Protocols are implemented to use quantum uncertainty and enable the parties to share a secure key. Contrary to classical channel, the laws of physics imply that any eavesdropper listening to the quantum transmission will modify this transmission and be detected. Quantum key distribution protocols may use different quantum measurements to lead to complex protocols, e.g., continuous variables protocols. The protocols used in the present work is built from the original discrete variable BB84 protocol with improvements.

Sharing a secret key from a quantum transmission is possible, even in the presence of noise. One need to apply privacy amplification as a function of the observed quantum bit error rate (QBER) to generate a secret key between Alice and Bob. The security of QKD methods may then be guaranteed below maximum threshold, QBER $< 11.5\%$. Practicaly,

imperfect devices open also a security breach. For example, imperfect single photon sources such as fainted laser source, lead to an information leak due to multiphoton pulses. An eavesdropper may steal the extra photons on the channel without being discovered. The better possible attack in the photon number splitting attack (PNS). It implies a maximum transmission distance for Alice, as a function of her initial average energy per pulse. Therefore, QKD systems are required to use low energy level around 0.1-0.2 photon per pulse, to make the leaked information very small. For a transmission over standard monomode optical fiber and 0.2 photons per pulse, it is not possible to transmit a secure key beyond the maximum distance d_0 of about 62 km.

The variables used to encode the information in the photons are mainly polarization and phase. The principle used by most apparatus relies on the relative phase difference between two time separated pulses, like in a very long interferometer. To remove sensitivity over time to physical fluctuations, the QKD system developed at GTL-CNRS Telecom uses the SSB principle. The information encoding relies on the relative phase difference between a main peak and its modulation side bands, i.e., the relative phase difference between signals at different frequencies. The photon detection on one or the other modulation sideband enables implementation on the BB84 protocol. The SSB principle was easily implemented with standard off the shelf equipment such as MZIs or Fabry-Pérot filters.

The SSB principle security regarding resistance to transmission noise is inherited from general quantum key transmission systems. As for standard QKD systems, it is not possible to extract a secret key from the communication with over 11.5% QBER. We showed that the presence of the central peak in our scheme, which is always present and with high energy, may be considered as a *strong reference*. This signal guarantees the presence of a pulse. Theoretically, the protocol we use now is a *BB84 with reference* protocol, where the reference needs to be detected for each sent pulse. We showed by using a matrix format for the modulation phenomena that this reference may exist in the pulse without energy on the side pulses that carry information. Although, our system uses a fainted laser source as single photon source approximation, the strong reference makes the system resistant to the

PNS attack. It prevents an eavesdropper from blocking the pulses or from creating a *zero photon* signal that would present the reference but no information signal.

The SSB system is secure for any distance and is not limited to d_0. The energy that maximizes the secure bit rate is one photon per pulse. This is a great improvement compared to the commonly used 0.1 photon per pulse in current systems.

The built prototype enables transmission for distances over eighty kilometers. The light path fluctuations auto-compensation system that we have implemented makes our system very stable to the physical constraints on the transmission channel. We implemented this autocompensation thanks to standard WMD technology components. Such devices reduce the cost and the system benefits from their stability. Quantum key distribution use in the third telecom window (1550 nm) opens the doors of high speed secure communication with WDM technology for quantum cryptography.

The implemented automation showed a very strong stability. The computer control of encoding variables enabled transmission over long period of time. The automation also enables transmission of large keys, many megabytes in size, over tens of kilometers. The observed performance for optical fiber spools, as well as for deployed fiber, validates the principle on operational networks. The obtained rate and performance for stability of our prototype lead one to consider this system to be implemented in an industry that need hypersecure transmission over optical fibers.

The improvement on the system will incrementally enhance the existing prototype. The current weakest point is the single photon detection. Detectors at 1550nm are avalanche photodiodes with a 10-12% efficiency. A big step forward would be to find some new materials to detect single photon energy levels or to use frequency converter to use efficient detectors. A much higher efficiency would greatly lower the quantum error rate. This would also enable the implementation of protocols more efficiently, but cause them to be more sensitive to transmission errors.

The short term perspectives include the use of new communication protocols. It would

be possible to transmit directly a message in the quantum channel. The strong reference presence in the pulse would be used as well for continuous variable systems with homodyme detection [30].

There is probably purpose and meaning in our journey, but it is the pathway that is worth our while. Karin Boye.

REFERENCES

[1] Acín, A., Gisin, N., and Scarani, V., "Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks," *Phys. Rev. A*, vol. 69, no. 1, p. 012309, 2004.

[2] Agrawal, G. P., *Fiber-Optic Communication Systems*. John Wiley & Sons, 2002.

[3] Aspelmeyer, M., Jennewein, T., Pfennigbauer, M., Leeb, W. R., and Zeilinger, A., "Long-distance quantum communication with entangled photons using satellites," *Jour. of Sel. Top. in Quant. Elec.*, vol. 6, no. 6, pp. 1441–1451, 2003.

[4] Bechmann-Pasquinucci, H. and Gisin, N., "Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography," *Phys. Rev. A*, vol. 59, pp. 4238–4248, June 1999.

[5] Bennett, C. H., "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, pp. 3121–3124, May 1992.

[6] Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., and Smolin, "Experimental quantum cryptography," *J. Crypto.*, vol. 5, no. 1, pp. 3–28, 1992.

[7] Bennett, C. H. and Brassard, G., "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE International Conference Computers, Systems and Signal Processing, Bangalore, India*, pp. 175–179, IEEE, New York, 1984.

[8] Bennett, C. H., Brassard, G., and Mermin, N. D., "Quantum cryptography without Bell's theorem," *Phys. Rev. Lett.*, vol. 68, pp. 557–560, Feb. 1992.

[9] Biham, E., Boyer, M., Brassard, G., van de Graaf, J., and Mor, T., "Security of quantum key distribution against all collective attacks," *Algorithmica*, vol. 34, pp. 372–388, Nov. 2002.

[10] Brandt, H. E., "Positive operator valued measure in quantum information processing," in *Proceedings of SPIE - The International Society for Optical Engineering*, vol. 3385, (Orlando, FL, USA), pp. 23–35, 1998.

[11] Breguet, J., Muller, A., and Gisin, N., "Quantum cryptography with polarized photons in optical fibres experiment and practical limits," *Jour. of Modern Optics*, vol. 41, pp. 2405–2412, Dec 1994.

[12] Burdell, G. P., "A Georgia Tech tradition," *Technique*, vol. 15, p. 12, 1927.

[13] Buttler, W. T., Hughes, R. J., Lamoreaux, S. K., Morgan, G. L., Nordolt, J. E., and Peterson, C. G., "Free-space quantum-key distribution," *Phys. Rev. A*, vol. 57, p. 2379, Apr. 1998.

[14] Buttler, W. T., Hughes, R. J., Lamoreaux, S. K., Morgan, G. L., Nordolt, J. E., and Peterson, C. G., "Practical free-space quantum key distribution over 1 km," *Phys. Rev. Lett.*, vol. 81, p. 3283, Oct. 1998.

[15] Buttler, W. T., Lamoreaux, S. K., Torgerson, J. R., Nickel, G. H., Donahue, C. H., and Peterson, C. G., "Fast, efficient error reconciliation for quantum cryptography," *Phys. Rev. A*, vol. 67, no. 5, p. 052303, 2003.

[16] Cerf, N. J., Levy, M., and Assche, G. V., "Quantum distribution of gaussian keys using squeezed states," *Phys. Rev. A*, vol. 63, no. 5, p. 052311, 2001.

[17] Cirac, J. I. and Gisin, N., "Coherent eavesdropping strategies for the four state quantum cryptography protocol," *Phys. Rev. A*, vol. 229, pp. 1–7, April 1997.

[18] Courtois, N. T. and Pieprzyk, J., "Cryptanalysis of block ciphers with overdefined systems of equations," in *Asiacrypt 2002*, pp. 267–287, 2002.

[19] Csiszar, I. and Körner, J., "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. IT-24, no. 3, pp. 339–348, 1978.

[20] Daemen, J. and Rijmen, V., *The Design of Rijndael*. Springer-Verlag, 2002.

[21] de Vigenere, B., *Traité des chiffres, ou secrètes manières d'escrire*. Paris, 1596.

[22] Duraffourg, L., Merolla, J.-M., Goedgebuer, J.-P., Mazurenko, Y., and Rhodes, W. T., "Compact transmission system using single-sideband modulation of light for quantum cryptography," *Opt. Lett.*, vol. 26, pp. 1427–1429, Sept. 2001.

[23] Einstein, A., Podolsky, B., and Rosen, N., "Can quantum-mechanical description of physical reality be considered complete?," *Physical Review*, vol. 47, pp. 777–780, May 1935.

[24] Ekert, A. K., "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug. 1991.

[25] Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H., "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, Jan. 2002.

[26] Gisin, N. and Wolf, S., "Quantum cryptography on noisy channels: Quantum versus classical key-agreement protocols," *Phys. Rev. Lett.*, vol. 83, no. 20, pp. 4200–4203, 1999.

[27] Gobby, C., Yuan, Z., and Shields, A. J., "Quantum key distribution over 122 km of standard telecom fiber," *Applied Physics Letters*, vol. 84, pp. 3762–3764, May 2004.

[28] Gottesman, D. and Preskill, J., "Secure quantum key distribution using squeezed states," *Phys. Rev. A*, vol. 63, no. 2, pp. 022309–1–022309–18, 2001.

[29] Gourdon, X., *Les maths en tête Algèbre*. Ellipses, 1994.

[30] Grosshans, F. and Grangier, P., "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, no. 5, p. 057902, 2002.

[31] Grosshans, F., van Assche, G., Wenger, J., Brouri, R., Cerf, N. J., and Grangier, P., "Quantum key distribution using gaussian-modulated coherent states," *Nature*, vol. 421, pp. 238–241, Jan. 2003.

[32] Guerreau, O. L., Malassenet, F. J., McLaughlin, S. W., and Merolla, J.-M., "Quantum key distribution without a single-photon source using a strong reference," *IEEE Photon. Technol. Lett.*, vol. 17, no. 8, pp. 1755–1758, 2005.

[33] Guerreau, O. L., Malassenet, F. J., McLaughlin, S. W., and Merolla, J.-M., "Enhanced throughput for QKD: A multiplexed approach," *IEEE J. Select. Topics Quantum Electron.*, 2006. Submitted.

[34] Guerreau, O. L., McLaughlin, S. W., Malassenet, F. J., and Merolla, J.-M., "Time domain single side pulse interference quantum key distribution scheme," in *ECOC'05, 31st European Conference on Optical Communication*, 2005.

[35] Guerreau, O. L., Merolla, J.-M., Soujaeff, A., Patois, F., Goedgebuer, J.-P., and Malassenet, F. J., "Long-distance QKD transmission using single sideband detection scheme with WDM synchronization," *IEEE J. Select. Topics Quantum Electron.*, vol. 9, pp. 1533–1540, November/December 2003.

[36] Hillery, M., "Quantum cryptography with squeezed states," *Phys. Rev. A*, vol. 61, no. 2, p. 022309, 2000.

[37] Hughes, R. J., Morgan, G. L., and Peterson, C. G., "Quantum key distribution over a 48km optical fibre network," *Jour. of Modern Optics*, vol. 47, pp. 533–547, Feb. 2000.

[38] Hughes, R. J., Nordholt, J. E., Derkacs, D., and Peterson, C. G., "Practical free-space quantum key distribution over 10 km in daylight and at night," *New J. Phys.*, vol. 4, pp. 43.1–43.14, July 2002.

[39] Huttner, B. and Ekert, A. K., "Information gain in quantum eavesdropping," *Jour. of Modern Optics*, vol. 41, pp. 2455–2466, Dec. 1994.

[40] Huttner, B., Imoto, N., Gisin, N., and Mor, T., "Quantum cryptography with coherent states," *Phys. Rev. A*, vol. 51, pp. 1863–1869, Mar. 1995.

[41] Inoue, K., Waks, E., and Yamamoto, Y., "Differential-phase-shift quantum key distribution using coherent light," *Phys. Rev. A*, vol. 68, no. 2, p. 022317, 2003.

[42] Inoue, K., Waks, E., and Yamamoto, Y., "Differential phase shift quantum key distribution," *Phys. Rev. Lett.*, vol. 89, no. 3, p. 037902, 2002.

[43] Kerckhoffs, A., "La cryptographie militaire," *Journal des sciences militaires*, vol. IX, pp. 5–83,161–191, Jan.Feb. 1883.

[44] Kosaka, H., Tomita, A., Nambu, Y., Kimura, T., and Nakamura, K., "Single-photon interference experiment over 100 km for quantum cryptography system using a balanced gated-mode photon detector," *Electronics Letters*, vol. 39, pp. 1199–1201, Aug. 2003.

[45] Kurtsiefer, C., Zarda, P., M.Halder, andPaul R. Tapster, P. M. G., Rarity, J., and Weinfurter, H., "Long-distance free-space quantum cryptography," in *Proceedings of SPIE*, vol. 4917, pp. 25–31, SPIE, Oct. 2002.

[46] Lütkenhaus, N., "Security against individual attacks for realistic quantum key distribution," *Phys. Rev. A*, vol. 61, pp. 052304–1:10, May 2000.

[47] Mayers, D., "Unconditional security in quantum cryptography," *Jour. of the ACM*, vol. 48, pp. 351–406, May 2001.

[48] Merolla, J.-M., Duraffourg, L., Goedgebuer, J.-P., Soujaeff, A., Patois, F., and Rhodes, W. T., "Integrated quantum key distribution system using single sideband detection," vol. 18, no. 2, pp. 141–146, 2002.

[49] Merolla, J.-M., Mazurenko, Y., Goedgebuer, J.-P., Duraffourg, L., Porte, H., and Rhodes, W. T., "Quantum cryptographic device using single-photon phase modulation," *Phys. Rev. A*, vol. 60, pp. 1899–1905, Sept. 1999.

[50] Muller, A., Greguet, J., and Gisin, N., "Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km," *Europhysics Letters*, vol. 23, pp. 383–388, Aug. 1993.

[51] Muller, A., Zbinden, H., and Gisin, N., "Quantum cryptography over 23 km in installed under-lake telecom fibre," *Europhysics Letters*, vol. 33, pp. 335–339, Feb. 1996.

[52] Nielsen, M. A. and Chuang, I. L., *Quantum Computation and Quantum Information*. Cambridge university Press, 2000.

[53] Peres, A., *Quantum Theory: Concepts and Methods*. Kluwer Academic Publisher, 1995.

[54] Proakis, J. G., *Digital Communications*. McGraw-Hill Book Co., 3rd ed., 1995.

[55] Rarity, J. G., Gorman, P. M., Wall, T. E., and Tapster, P. R., "Free-space quantum cryptography and satellite key uploading," in *IQEC, International Quantum Electronics Conference Proceedings*, 2000.

[56] Rivest, R. L., Shamir, A., and Adleman, L. M., "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120–126, Feb. 1978.

[57] Scarani, V., Acín, A., Ribordy, G., and Gisin, N., "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Phys. Rev. Lett.*, vol. 92, p. 057901, 2004.

[58] Schneier, B., *Applied Cryptography*. John Wiley & Sons, 1996.

[59] Shannon, C. E., "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, pp. 379–423 and 623–656, July and Oct. 1948.

[60] Shannon, C. E., "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, pp. 656–715, Oct. 1949.

[61] Shor, P. W., "Algorithms for quantum computation: discrete logarithms and factoring," in *35th Annual Symposium on Foundations of Computer Science*, pp. 124–134, 1994.

[62] Shor, P. W. and Preskill, J., "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, pp. 441–444, July 2000.

[63] Stücki, D., Gisin, N., Guinnard, O., Ribordy, G., and Zbinden, H., "Quantum key distribution over 67 km with a plug&play system," *New J. Phys.*, vol. 4, pp. 41.1–41.9, July 2002.

[64] Thangaraj, A., "Completely secure error correction in QKD systems." Private Report, 2003.

[65] Townsend, P. D., Rarity, J. G., and Tapster, P. R., "Enhanced single photon fringe visibility in a 10 km-long prototype quantum cryptography channel," *Electronics Letters*, vol. 29, pp. 1291–1293, July 1993.

[66] Townsend, P. D., Rarity, J. G., and Tapster, P. R., "Single photon interference in 10 km long optical fibre interferometer," *Electronics Letters*, vol. 29, pp. 634–635, Apr. 1993.

[67] Turing, A. M., *Mathematical theory of ENIGMA machine.* Public Record Office, London, 1940.

[68] Vernam, G. S., "Cipher printing telegraph systems for secret wire and radio telegraphic communications," *Journal of the American Institute of Electrical Engineers*, vol. 45, pp. 109–115, 1926.

[69] von Neumann, J., *Mathematische Grundlagen der Quantenmechanik.* Springer Verlag, 1932.

[70] Watterson, B., *Homicidal Psycho Jungle Cat.* Andrews McMeel Publishing, 1994.

[71] Wegman, M. N. and Carter, J. L., "New hash functions and their use in authentication and set equality," *Journal of Computer and System Sciences*, vol. 22, pp. 265–279, June 1981.

[72] Welsh, D., *Codes and Cryptography.* Clarendon Press, Oxford, 1988.

[73] Wiesner, S., "Conjugate coding," *SIGACT News*, vol. 15, no. 1, pp. 78–88, 1983. Manuscrit written *circa* 1970, unpublished until 1983.

[74] Wooters, W. K. and Zurek, W. H., "A single quanta cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[75] Yuan, Z., Gobby, C., and Shields, A. J., "Quantum key distribution over distances as long as 101km," in *CLEO/QELS 2003*, 2003.

Multidimensional Quantum Key Distribution with Single Side Pulse and Single Side Band Modulation Multiplexing

Olivier L. Guerreau-Lambert

128 Pages

Directed by Dr. Steven W. McLaughlin and Dr. François J. Malassenet

Quantum Cryptography enables secret distribution between remotes parties where classical communications fail. The proposed technique uses optical signal modulation to encode information with relative phase difference between frequency separated signals. The single side band detection scheme (SSB) enables efficient secret key distribution. The system security is guaranteed with a strong reference protocol. One can use a fainted laser source without security breach for any distance. A second proposed technique uses relative phase difference between time separated pulses. The single side pulse detection scheme (SSP) enables efficient secret key distribution and benefits the same security features as the SSB system. Both SSP and SSB may be multiplexed to increase the secure bit rate. The maximizing initial average energy is then one photon per pulse. The implemented SSB protocol includes an autocompensation system for the optical path fluctuations that make the system robust over long time periods.